Universitetet i Stavanger

DET TEKNISK-NATURVITENSKAPELIGE FAKULTET

MASTEROPPGAVE

Studieprogram/spesialisering: MSAMAS Master i Samfunnssikkerhet	Vårsemesteret, 2019 **Åpen** / ~~Konfidensiell~~
Forfatter: Torbjørn Størdal Nilsen	Torbjørn Størdal Nilsen ..... (signatur forfatter)
Fagansvarlig: Ole Andreas Hegland Engen **Veileder:** Morten Sommer	
Tittel på masteroppgaven: Cybersikkerhet i nettselskap. En studie av cybersikkerhet i et menneskelig og organisatorisk perspektiv **Engelsk tittel:** Cyber Security in Network Companies. A Study of Cyber Security, From a Human and Organizational Perspective	
Studiepoeng: 30	
Emneord: Cybersikkerhet, IKT-sikkerhet, barrierer, informasjonssikkerhet, risikostyring, MTO, HRO, mindfulness, kollektiv bevissthet, nettselskap.	**Sidetall:71** + vedlegg/annet: 79 **Stavanger, 15.06.2019**

Forside for masteroppgave

Universitetet
i Stavanger

Cybersikkerhet i nettselskap

En studie av cybersikkerhet i et menneskelig og organisatorisk perspektiv

Masteroppgave i samfunnssikkerhet

Universitetet i Stavanger

Vår 2019

Forfatter: Torbjørn Størdal Nilsen

Veileder: Morten Sommer

Forord

Denne masteroppgaven markerer slutten på to spennende år ved Universitet i Stavanger på samfunnssikkerhetsstudiet. Arbeidet med masteroppgaven har vært en krevende og givende prosess som har gitt meg muligheten til å lære om både cybersikkerhet og kraftbransjen.

Først og fremst ønsker jeg å rette en stor takk til alle respondenter fra nettselskapene som har tatt seg tid til intervju. Mange har sagt nei, mens andre har trukket seg. Denne oppgaven hadde derfor ikke vært mulig å gjennomføre uten at dere ønsket å dele deres kunnskap med meg.

Jeg vil også takke min veileder Morten Sommer for konstruktive tilbakemeldinger og for å alltid ha troen på prosjektet.

Takk til alle kjente og kjære som har gjort tilværelsen i Stavanger så minnerik. Spesielt stor takk til Lisa for all støtte og faglige innspill gjennom arbeidet med masteroppgaven.

Til slutt vil jeg takke mine foreldre for deres hjelp og støtte hver gang jeg har trengt det.

Torbjørn Størdal Nilsen

Stavanger, 13.06.2019

Sammendrag

Stabil energiforsyning er en kritisk infrastruktur som øvrige samfunnsfunksjoner er fullstendig avhengig av. Kraftbransjen har som resten av samfunnet blitt mer digitalisert og avhengig av IKT-baserte løsninger. Digitalisering og stadig flere komponenter tilknyttet internett har imidlertid medført at energisektoren eksponeres for en rekke nye cybertrusler. Cybersikkerhet har tradisjonelt vært en teknisk disiplin med mange tekniske løsninger tilgjengelig. Ofte viser det seg imidlertid at tekniske løsninger alene ikke er tilstrekkelig. Formålet med denne studien har vært å undersøke cybersikkerhet i kraftsektoren fra et ikke-teknologisk perspektiv. Denne studien undersøker hvilke ikke-tekniske barrierer som benyttes av nettselskapene, og hvilken effekt de mener barrierene har på cybersikkerheten. På bakgrunn av dette er følgende problemstilling lagt til grunn:

«Hvordan forstår nettselskaper betydningen av ikke-tekniske barrierer innen cybersikkerhet?»

For å svare på problemstillingen har IKT-sikkerhetsledere og øvrige sikkerhetsledere i tre nettselskap blitt intervjuet om hvordan de forstår de menneskelige og organisatoriske forholdenes innvirkning på cybersikkerheten, og hvilke barrierer som benyttes i dette sikkerhetsarbeidet. Funnene har blitt drøftet opp mot teori basert på risikostyring og barrierer, MTO-perspektivet, med ekstra fokus på den menneskelige faktor og organisatoriske ulykker, og kollektiv bevissthet (mindfulness).

Resultatene viser at nettselskapene bruker en rekke ulike ikke-tekniske barrierer innenfor cybersikkerhet, og at nettselskapene forstår cybersikkerhet som en kombinasjon av ikke-tekniske og tekniske barrierer. De ikke-tekniske barrierene er spesielt viktige innenfor opplæring og bevisstgjøring. I tillegg er det eksempler på at regler, rutiner og prosedyrer er viktige for å støtte opp om funksjonaliteten til tekniske barrierer. Samtidig har ikke-tekniske barrierer sine klare begrensninger ettersom de er avhengig av at de ansatte tolker og forstår hvordan barrierene skal iverksettes i praksis. Nettselskapenes forståelse av menneskelige feilhandlinger peker i retning av forklaringer ved organisasjonen og miljøet de ansatte opererer i, heller enn karakteristikker med de ansatte selv. Dette gjenspeiles i nettselskapenes barrierestyring gjennom at flere av barrierene er satt inn for å redusere risikoen for feilhandlinger og øke feiltoleransen, samt prioriteringen av opplæring. Nettselskapenes kollektive bevissthet er avgjørende for at ikke-tekniske barrierer skal fungere. Karakteristikker som utgjør kollektiv bevissthet observeres imidlertid blant nettselskapene. Dette kan tyde på at nettselskapene er årvåkne i møte med cybertrusler, noe som påvirker barrierenes pålitelighet.

Innholdsfortegnelse

1. Innledning

Digitaliseringen har de siste tiårene ført til gjennomgripende samfunnsmessige endringer på tvers av sektorer. Kritisk infrastruktur blir stadig mer avhengig av informasjons- og kommunikasjonsteknologi (IKT) for å fungere. IKT-systemer benyttes i dag for å drifte, overvåke og fjernstyre anleggene i energiforsyningen (NOU, 2015). IKT har blitt en viktig del av energiforsyningen for å kunne tilfredsstille samfunnets krav til effektiv drifts- og forsyningssikkerhet. Den økte digitaliseringen av energisektoren har imidlertid medført at bransjen er mer utsatt for cybertrusler. Undersøkelser fra Norges vassdrags- og energidirektorat (NVE) viser at 70% av de spurte virksomhetene i kraftbransjen har hatt uønskede IT-sikkerhetshendelser siste året. Hendelsene omfatter blant annet hacking, dataskadeverk, virus og malware-infeksjon (NVE, 2017a). Nasjonal sikkerhetsmyndighet (NSM) observerer i sin årlige trusselvurdering i 2017 at det er en jevn økning i antall cyberangrep mot norske virksomheter. NSM ser tegn på økt bevissthet om teknisk sårbarhet, men gjennomføringen sikkerhetstiltak skjer ikke i samme takt som utviklingen av trusselbildet (NSM, 2017).

Internasjonalt har det vært flere større cyberangrep som har ført til økt oppmerksomhet om det digitale risikobildet. Den kjente skadelige datamaskinormen «Stuxnet» beviste i 2010 at det var mulig å angripe kontrollsystemer som Supervisory Control and Data Acquisition (SCADA) og faktisk påføre fysisk ødeleggelse. Angrepet saboterte atomanrikningsanlegget i byen Natanz i Iran (Hamnes, 2010). I 2015 ble et ukrainsk elektrisitetsdistribusjonsfirma (Kyivoblenergo) rammet av et cyberangrep rettet mot SCADA-systemene. Angrepet medførte at rundt 230.000 kunder mistet strømmen (Frøystad, 2017). Som observert i Ukraina kan cyberangrep i verste fall føre til stans i strømtilførselen. Avbrutt strømforsyning vil få store konsekvenser på tvers av sektorer ettersom samfunnet er fullstendig avhengig av stabil energiforsyning. 19. mars 2019 fikk cyberangrep nasjonal oppmerksomhet da Hydro oppdaget at de var rammet av et løspengevirus. Viruset krypterte informasjonen på selskapets datamaskiner, og det ble lagt fram krav om betaling for å få informasjonen låst opp igjen. Som følge av angrepene måtte Hydro stenge produksjonen ved flere anlegg. Kostnaden på angrepet er estimert til å ha vært 300-350 millioner kroner (Stavanger Aftenblad, 2019).

Cybersikkerhet blir stadig mer aktuelt i kraftbransjen. Kraftbransjens eget sikkerhetsselskap, *KraftCERT*, hevder at angrepet som skjedde i Ukraina kan være mulig å gjennomføre i Norge (Johansen, 2016). Politiets sikkerhetstjeneste (PST) forventer at flere lands etterretningstjenester vil forsøke å kartlegge sårbarheter i norsk kritisk infrastruktur (PST, 2019). På bakgrunn av det dynamiske risikobildet er det viktig at virksomhetene i kraftsektoren arbeider gjennom en systematisk og helhetlig tilnærming til cybersikkerhet. Cybersikkerhet har tradisjonelt vært en teknisk disiplin med mange tekniske løsninger tilgjengelig (Albrechtsen & Hovden, 2011) Cybersikkerhet er, og vil alltid være en teknisk disiplin. Uten tekniske sikkerhetsløsninger ville hvert eneste datasystem kollapset. Cybersikkerhet er imidlertid ikke bare et teknisk fenomen, ettersom teknologien er høyst avhengig av menneskene og organisasjonen som disponerer den (Albrechtsen & Hovden 2011, Line & Tøndel, 2012).

Menneskelig feil og manglende sikkerhetsbevissthet bidrar til at uønskete IKT-hendelser oppstår (NVE, 2017a). «*Mennesket er det svakeste leddet*» er et kjent uttrykk (NOU, 2015). Hackere forsøker å manipulere mennesker gjennom å lure dem til å trykke på skadelige lenker i eposter («*phishing*»), og laste ned ondsinnet programvare. Det er dokumentert at svak ledelse, menneskelige feilhandlinger, manglende sikkerhetsbevissthet, samt organisatoriske forhold er bidragsytere til at uønskete hendelser oppstår i IKT-systemer (NOU, 2015). Det er derfor viktig at virksomhetene kompenserer for menneskelig og teknologisk sårbarhet gjennom en helhetlig tilnærming til cybersikkerhet. I dette arbeidet er både tekniske og ikke-tekniske virkemidler tilgjengelig (Albrechtsen & Hovden, 2011). Denne studien vil omhandle de ikke-tekniske tiltakene.

1.1 Problembeskrivelse

Stabil energiforsyning er en kritisk infrastruktur som øvrige samfunnsfunksjoner er fullstendig avhengig av. Kraftbransjen har som resten av samfunnet blitt mer digitalisert og avhengig av IKT-baserte løsninger. Digital teknologi benyttes til å kontrollere energiproduksjon og distribusjon, samt overføre informasjon om forbruk og etterspørsel (NVE, 2017a). IKT har gitt virksomhetene en mulighet til å utvikle løsninger for smarte energiøkonomiske hus og mer effektiv drift. Digitalisering og stadig flere komponenter tilknyttet internett har imidlertid medført at energisektoren eksponeres for en rekke nye cybertrusler (NVE, 2017a). SCADA-systemer og andre IKT-system som benyttes innenfor energidistribusjon har blitt sårbare ovenfor cyberangrep (NOU, 2015). Introduksjonen av IKT inn i systemer som tidligere har vært

driftet manuelt har ført til at en nå må ta hensyn til hendelser som er forårsaket av ondsinnete aktører. Tidligere måtte en være geografisk lokalisert nært systemene for å påføre dem skade, mens nå som systemene er koblet opp mot internett kan en i teorien få tilgang til systemene fra en hvilken som helst posisjon (NOU, 2015, Skotnes, 2015).

Norske virksomheter i kraftsektoren rapporterer at det forekommer uønskete IT-sikkerhetshendelser. Hendelsene omfatter hovedsakelig dataskadeverk, bedrageri, virus-infeksjon, forsøk på datainnbrudd og hacking (NVE, 2017a). Angrepene kan blant annet være økonomisk og politisk motiverte (etterretning, sabotasje og cyberkriminalitet), men kan også være vandalisme utført av privatpersoner (NOU, 2015). Tidligere undersøkelser har konkludert med at manglende sikkerhetsbevissthet hos ansatte, menneskelig feil og at eksisterende prosesser ikke ble fulgt, utgjør hovedandelen av de medvirkende faktorene til at hendelsen oppstod (NVE, 2017). Forskningen på cybersikkerhet har tradisjonelt vært dominert av de tekniske fagdisiplinene (Siponen & Oinas-Kukkonen, 2007). Det viser seg imidlertid at tekniske løsninger alene ikke er tilstrekkelig, ettersom mange av angrepene lykkes på grunn av at mennesker manipuleres til å begå feil (NOU, 2015). Det er eksempelvis mennesker som utøver utilstrekkelig sikkerhetsadferd når de lager for enkle passord. Det er også mennesker som lar seg lure av hackere når de trykker på lenker i e-poster som inneholder skadevare. De fleste gjør imidlertid ikke disse feilene intensjonelt. Årsaken til feilene kan være mange, alt fra manglende bevissthet om risiko, utilstrekkelig opplæring eller høyt arbeidspress (NOU, 2015).

Formålet med denne studien er å undersøke cybersikkerhet i kraftsektoren fra et ikke-teknologisk perspektiv. Studien vil belyse hvordan organisatoriske og menneskelige forhold påvirker cybersikkerhet. Nærmere bestemt ønskes det med denne studien å undersøke hvilke ikke-tekniske barrierer som benyttes av nettselskapene, og hvilken effekt de mener barrierene har på cybersikkerheten. På bakgrunn av dette er følgende problemstilling lagt til grunn:

Hvordan forstår nettselskaper betydningen av ikke-tekniske barrierer innen cybersikkerhet?

For å svare på problemstillingen vil IKT-sikkerhetsledere og øvrige sikkerhetsledere i ulike nettselskap intervjues om hvordan de forstår de menneskelige og organisatoriske forholdenes innvirkning på cybersikkerheten, og hvilke barrierer som benyttes i dette sikkerhetsarbeidet. En barriere vil i denne studien forstås som enhver sikkerhetsfunksjon som har som mål å forhindre

ulykker inklusivt prosedyrer og opplæring. (Rosness, Guttormsen, Steiro, Tinnmansvik & Herrera, 2002). James Reason (1997) skiller mellom harde og myke barrierer. Harde barrierer kan være fysisk sikring av verdier, og teknologiske sikkerhetsløsninger (Brannmur, antivirus, kryptering). I denne studien vil det fokuseres på de myke barrierene. Myke barrierer består av en blanding av mennesker og papirer. Eksempler på myke barrierer kan være trening, opplæring, regler og prosedyrer, sikkerhetsinstrukser. (Reason, 1997). I denne studien er det også valgt å inkludere ROS-analyser, som er et sentralt verktøy i å planlegge og velge barrierer (Aven, 2017), samt ulike former for beredskapsøvelser som også kan bidra til å forbedre barrierene (Engen, Kruke, Lindøe, Olsen, Olsen og Pettersen, 2016). Alt dette velger jeg å kalle for ikke-tekniske barrierer ettersom dette er barrierer som først og fremst er avhengig av mennesker, ikke teknologi.

For å kunne undersøke hvordan nettselskapene forstår betydningen av barrierer, er det nødvendig å undersøke hvilke ikke-tekniske barrierer som benyttes og hvilken funksjon de har innenfor nettselskapenes cybersikkerhet. Mennesker utgjør en viktig del av cybersikkerhetsarbeidet i et digitalisert samfunn, og derfor er det interessant å undersøke hvordan nettselskapene forstår menneskelig feilhandlinger og hvordan dette påvirker valg av barrierer innen cybersikkerhet. Weick, Sutcliffe & Obstfeld, (1999) opererer med begrepet kollektiv bevissthet (mindfulness) om sentrale karakteristikker med høypålitelige organisasjoner (HRO). Disse karakteristikkene bidrar til at organisasjoner klarer å oppnå pålitelighet i et dynamisk risikobilde. Det kan dermed tenkes at nettselskapenes kollektive bevissthet vil påvirke påliteligheten til de ikke-tekniske barrierene.

I denne forbindelse er det utarbeidet tre forskningsspørsmål for å svare på problemstillingen «*Hvordan forstår nettselskaper betydningen av ikke-tekniske barrierer innen cybersikkerhet?*»:

1. Hvordan bruker nettselskapene ikke-tekniske barrierer, og hvilken funksjon har barrierene i nettselskapenes cybersikkerhet?

2. Hvilken betydning har nettselskapenes forståelse av menneskelige feilhandlinger for barrierestyring innen cybersikkerhet?

3. Hvilken betydning har nettselskapenes kollektive bevissthet på ikke-tekniske barrierers pålitelighet innen cybersikkerhet?

1.2 Avgrensninger

Arbeidet med cybersikkerhet i kraftsektoren er omfattende og involverer mange ulike aktører. På grunn av tids- og ressursbegrensninger er det nødvendig å foreta noen avgrensninger ettersom en studie av hele cybersikkerhetsarbeidet til kraftsektoren blir for omfattende. I denne studien velges det å studere nettselskaper. God cybersikkerhet er relevant for hele bransjen, men med tanke på forsyningssikkerhet er det nettselskaper som er det mest sårbare leddet i strømforsyningen (Skotnes, 2015). Myndighetene er en sentral og viktig del av sikkerhetsarbeidet i kraftsektoren. Regulering og tilsynsutøvelse er viktige virkemidler i arbeidet med sikkerhet i kraftsektoren. I denne studien er det imidlertid valgt å fokusere på nettselskapenes interne sikkerhetsarbeid. Myndighetenes tilsynsutøvelse og regulering vil dermed ikke drøftes i denne studien, selv om sikkerhetsarbeidet til nettselskapene er sterkt påvirket av nettopp myndighetskrav og regulering. Rollen til underleverandører, eksterne samarbeidspartnere som andre IT-sikkerhetsfirma, samt outsourcing av enkelte IT-tjenester er heller ikke diskutert i denne oppgaven.

Ettersom studiens problemstilling omhandler ikke-tekniske barrierer vil ikke de tekniske barrierene (brannmurer, antivirus, kryptering osv.) undersøkes direkte. Fokuset er rettet mot hvilke menneskelige og organisatoriske faktorer og aktiviteter som påvirker cybersikkerheten. Tekniske og digitale løsninger blir dermed ikke undersøkt direkte, bare hvordan de indirekte påvirkes av ikke-tekniske barrierer. Istedenfor undersøkes det hvilke organisatoriske betingelser som må være til stede for at mennesker og teknologi sammen kan interagere trygt. Ettersom studien er avgrenset til ikke-tekniske barrierer vil heller ikke fysisk sikring av IKT, infrastruktur og analog informasjon drøftes selv om dette også en viktig del av cybersikkerheten.

1.3 Tidligere forskning

Følgende vises det til tidligere forskning som er relevant for denne studiens tematikk. Hagen, Albrechtsen & Hovden (2008) har forsket på effektiviteten til ulike organisatoriske informasjonssikkerhetstiltak. Resultatene viser at tiltak innen bevisstgjøring er de mest effektive av de organisatoriske virkemidlene. Innenfor kraftbransjen har doktorgradsarbeidet til Skotnes (2015) forsket på utfordringer for sikkerhetsstyring av IKT i nettselskaper. Resultatene viser blant annet at bruken av bevisstgjørings- og opplæringstiltak varierer stort

mellom nettselskapene, og at manglende bevissthet mot farer kan føre til svak årvåkenhet som gir et større potensial for at cyberangrep lykkes.

Røyksund (2011) sin masteravhandling om informasjonssikkerhet i kraftforsyningen fokuserer på risikopersepsjon for angrep mot driftskontrollsystem og hva som påvirker valg av informasjonssikkerhetstiltak. Masteravhandlingen til Kruke (2017) omhandler nettselskapers bruk av barrierer for å beskytte sensitiv informasjon, og hvordan de ansattes bevissthet påvirker barrierene. Line & Moe (2015) har forsket på nettselskapers bruk av beredskapsøvelser på IT-hendelser. Resultatene viser at slike øvelser bidrar til trening på praktisk samhandling, som leder til forbedret responskapasitet på IT-hendelser. Slike øvelser er imidlertid ikke spesielt utbredt i kraftbransjen.

I et felt med rask teknologisk utvikling og et dynamisk risikobilde er det nødvendig med mer forskning. Denne studien vil bidra til å belyse bruk av ikke-tekniske barrierer innenfor cybersikkerhet.

2. Kraftsektoren og cybersikkerhet

I dette kapittelet vil det kontekstuelle bakteppet for studien presenteres. Først redegjøres det for norsk kraftforsyning og hva som menes med et nettselskap. Dette inkluderer å gjennomgå sentrale begrep som SCADA-systemer og administrative nettverk. Deretter vil cybersikkerhetsbegrepet redegjøres for, samt en gjennomgang av ulike typer cyberhendelser. Avslutningsvis presenteres eksempler på cyberhendelser i kraftsektoren.

2.1. Norsk kraftforsyning og nettselskap

Omtrent 98,5% av norsk elektrisitetsdistribusjon produseres av vannkraftverk. Kraftnettet kan deles inn i tre nivå: sentral-, regional- og distribusjonsnett. Sentralnettet knytter sammen forbrukere, produsenter og overføringsledninger til utlandet. Regionalnettet er bindeleddet mellom sentralnettet og distribusjonsnettene. Distribusjonsnettene sørger for distribusjon av kraft til husholdninger, tjenesteytere og annen næringsvirksomhet (NOU, 2015). De største produksjonsanleggene knyttes til sentral- eller regionalnettet, mens de mindre produksjonsanleggene vil tilknyttes regional- eller distribusjonsnett (Energinorge, u.å.). Kraftleverandør er selskapet som en kjøper strøm i fra. Forbrukeren kan velge mellom ulike

leverandører, som alle har forskjellige priser og avtalevilkår, men en får den samme strømmen uansett hvilken kraftleverandør en velger (Energinorge, u.å.).

Et nettselskap er ansvarlig for å drifte strømnettet i et område, og å sørge for at strømmen fra kraftleverandøren blir transportert til sluttbrukeren. Nettselskapet har monopol på sine tjenester innenfor et geografisk område, og en kan i motsetning til kraftleverandør, ikke bytte nettselskap selv om en er misfornøyd med tjenestene deres. Forbrukeren må dermed betale det samme i nettleie til det lokale nettselskapet (Energinorge, u.å.). I Norge er det over 120 nettselskap, og enkelte selskaper eier både deler av sentralnettet og regionalnettet. Enkelte eier også distribusjonsnett (NVE, 2019b).

Nettselskapene reguleres av NVE som fastsetter årlige inntektsrammer, og setter en øvre begrensning på hvor mye selskapene kan ta betalt. Formålet med reguleringen er også at nettet skal driftes på en samfunnsmessig effektiv måte (NVE, 2019a). NVE er også beredskapsmyndighet for energiforsyningen, noe som innebærer å føre tilsyn med sikkerhet og beredskap (NVE, 2019b). Alle nettselskap må forholde seg til kraftberedskapsforskriften som inneholder en rekke krav til organiseringen av cybersikkerhet, og øvrig sikkerhet og beredskap (Beredskapsforskriften, 2012, §1-3).

2.1.1 SCADA-systemer og administrative system

I nettselskapenes drift av strømnettet kan en dele virksomhetens nettverk i SCADA-systemer (driftskonkontroll) og de administrative nettverk (kontornettverk). De administrative systemene omfatter alt som ikke er å betrakte som prosesskontrollsystemer. Dette inkluderer økonomistyring, handel, IT-drift, logistikk og kundestøtte og lignende. (NVE, 2017b). SCADA-system (driftskontrollsystemene) brukes for å kontrollere og overvåke prosesser i kraftproduksjon og nettdrift. SCADA-systemene har tradisjonelt vært isolerte systemer, hvor cyberangrep har vært nærmest umulig å gjennomføre. Gjennom utviklingen av smartgrid-teknologi de siste tiårene, kan en ikke lengre anta at det ikke finnes noen forbindelse til omverdenen (Jaatun, Moe, Nordbø, 2017). Etter hvert som systemene i stadig større grad har blitt koblet til andre IKT-system, har det blitt gjennomført et omfattende arbeid for å sikre systemene mot uautorisert tilgang (NOU, 2015).

I cyberangrepet i Ukraina 2015, klarte angriperne å få fjerntilgang til SCADA-systemene, og koble ut 27 nettstasjoner. Dette resulterte i strømbrudd for rundt 230.000 kunder. Angriperne skaffet seg tilgang gjennom å først kompromittere det administrative nettverket, gjennom målrettete phishing-eposter som inneholdt skadevare. Denne skadevaren ble brukt til å samle

inn brukernavn og passord som gjorde at angriperne kunne få tilgang til SCADA-systemer (Jaatum et al., 2017).

2.2 Cybersikkerhet

Denne studien er avgrenset til å omhandle cybersikkerhet. I dagligtalen benyttes begrepene cybersikkerhet, IKT-sikkerhet og informasjonssikkerhet ofte om hverandre. Begrepene har imidlertid ulik betydning, selv om det er betydelig overlapp mellom dem. Det er derfor nødvendig å definere cybersikkerhet, IKT-sikkerhet og informasjonssikkerhet, for å spesifisere studiens utgangspunkt og avgrensninger.

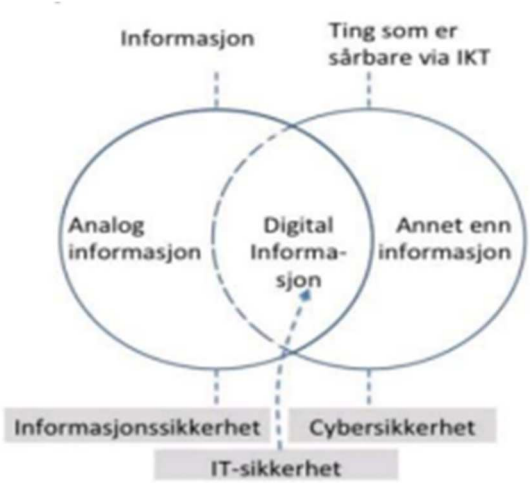
Begrepet cybersikkerhet beskriver beskyttelse av ting som er sårbare via IKT (NVE, 2017b). Både mennesker og fysiske komponenter kan være sårbar via IKT. SCADA-systemer som benyttes innen styring og overvåking av industrielle prosesser kan eksempelvis gis uautorisert tilgang til angripere via internett. Dette kan i verste fall få fysiske konsekvenser som f.eks. strømavbrudd, som igjen vil påvirke mennesker og næringsliv. Skadelig programvare kan dermed direkte skade infrastruktur og mennesker. «Stuxnet»-ormen som saboterte atomanlegg i Iran eksemplifiserer en sårbarhet via IKT som fikk fysiske konsekvenser.

Informasjonssikkerhet omhandler sikring av informasjon, uavhengig av om den er digital eller analogt lagret. Det er vanlig å definere informasjonssikkerhet til å omhandle elementene *konfidensialitet*, *integritet* og *tilgjengelighet*. *Konfidensialitet* handler om å sikre informasjon mot uvedkommende og sikre at kun autorisert personell har tilgang til denne informasjonen. *Integritet* handler om å sikre at informasjonen er fullstendig, nøyaktig og gyldig. *Tilgjengelighet* betyr at informasjonen skal være tilgjengelig når det trengs som f.eks. innebærer å støtte funksjoners stabilitet (NVE, 2017b).

IKT-sikkerhet omhandler sikring av informasjons- og kommunikasjonsteknologi, med andre ord maskinvare og programvare. Det er dermed selve teknologien som ønskes å beskyttes når man snakker om IKT-sikkerhet. Ofte benyttes imidlertid IKT-sikkerhet og informasjonssikkerhet om hverandre ettersom at mye informasjon er lagret via IKT. IT-sikkerhet betyr sikring av informasjonsteknologi, men i praksis er det ingen forskjell på IKT-sikkerhet og IT-sikkerhet (NVE, 2017b).

Rossouw von Solms og Johan van Niekerk (2013) argumenterer for at cybersikkerhetsbegrepet inneholder flere dimensjoner enn både informasjonssikkerhet og IKT-sikkerhet inneholder, og

at skillet mellom begrepene har etiske implikasjoner. Cybersikkerhet handler ikke nødvendigvis bare om å beskytte selve cyberspace, eller informasjonen i seg selv, men om å beskytte alt som er sårbart via IKT. Både mennesker og teknologi kan skades via sårbarheter i IKT. Dette kan selvfølgelig også være en konsekvens av brudd på informasjonssikkerhet og IKT-sikkerhet, men der vil skaden alltid være indirekte (von Solms & van Niekerk, 2013). En finner elementer av IKT-sikkerhet og informasjonssikkerhet i cybersikkerhetsbegrepet, som er et bredere begrep. For å sikre ting som er sårbare via IKT er det dermed naturlig å satse på IKT-sikkerhet. I tillegg vil den digitale delen av informasjonssikkerhetsbegrepet også dekkes av cybersikkerhetsbegrepet (NVE, 2017b).



Figur 1 viser sammenhengen mellom cybersikkerhet, IKT-sikkerhet og informasjonssikkerhet (NVE, 2017b).

I det norske språket er det bare ett etablert ord for sikkerhet. På engelsk skilles det imidlertid mellom safety og security, der førstnevnte omhandler ulykker, mens sistnevnte handler om ondsinnete handlinger (Engen et al., 2016). Safety henviser til risikoen knyttet til handlinger og hendelser som ikke har noen planlagt ondsinnet intensjon, som f.eks. industriulykker og naturkatastrofer. Security handler om risiko knyttet til tilsiktede uønskete handlinger som sabotasje, kriminalitet og terrorisme (Engen et al., 2016). Cybersikkerhet inkluderer elementer fra både safety og security ettersom et IKT-system vil reagere på samme måte om det er en tilsiktet, eller en utilsiktet handling som har utløst den samme uønskete hendelsen (Sivertsen, 2007). Ikke-tilsiktede hendelser kan være menneskelige feilhandlinger, fysisk svikt og naturhendelser som påfører svikt i IKT-systemene. Med tilsiktede hendelsene innenfor

cybersikkerhet menes angrep eller manipulasjon av et IKT-system (Sivertsen, 2007). Ettersom årsakskjedene og konsekvensene ofte blir de samme, uavhengig av opprinnelig årsak, innebærer sikkerhet for begge hendelsestypene mange av de samme egenskapene. Sårbarhetsreduserende tiltak kan dermed motvirke både tilsiktede og utilsiktede hendelser (Sivertsen, 2007).

En vesentlig forskjell er imidlertid at en ondsinnet aktør kan ha kapasitet til å tilpasse seg og forsere barrierer og sikringstiltak (Engen et al., 2016) Dette er en særskilt utfordring ved tilsiktede handlinger. Begrepet cybersikkerhet gir sterke assosiasjoner til tilsiktede handlinger, og store deler av litteraturen om datasikkerhet handler kun om sikkerhet knyttet til tilsiktede handlinger (Sivertsen, 2007). Følgende vises det til ulike eksempler på tilsiktede cyberangrep.

2.2.1 Tilsiktede cyberangrep

I takt med digitaliseringen av samfunnet utgjør cyberkriminalitet en stadig større risiko for norske virksomheter. Hvert andre år kartlegger Næringslivets Sikkerhetsråd (NSR) IT-sikkerhetsnivået i norske virksomheter gjennom Mørketallsundersøkelsen. NSR observerer en jevn økning i cyberangrep mot norske virksomheter (NSR, 2018). De minst teknisk avanserte truslene er såkalte «script kiddies» eller sosiale hackere. Dette er personer som kan søke økonomisk eller politisk innflytelse, mens andre tilsynelatende ikke har annet mål enn å gjøre vandalisme og få anerkjennelse (NOU, 2015). Cyberangrep blir imidlertid også gjennomført av profesjonelle aktører som benytter stadig mer sofistikerte angrepsmetoder. Det finnes blant annet egne kriminelle markeder der en kan kjøpe og selge «konsulenttjenester», der en selger både kompetanse og hackerverktøy (NVE, 2017b). Aktørene konkurrerer på god kvalitet og service som i det åpne kommersielle markedet, og kundene av slike tjenester kan være alt fra stater, organisasjoner, eller privatpersoner (NOU, 2015). Spesielt autoritære stater som Russland og Kina nevnes ofte i forbindelse med cyberangrep (PST, 2019). PST forventer at fremmede etterretningsoperasjoner vil utføres mot norske virksomheter (PST, 2019).

Det finnes mange ulike metoder for å angripe via IKT. Den vanligste metoden er infisert epost, phishing (nettfiske). Dette er en teknikk der en forsøker å sende en epost som framstår som relevant eller attraktiv for mottakeren, f.eks. gjennom å utforme eposten som om den er sendt fra en offentlig etat (NSR, 2018). Formålet er ofte å få mottakeren til å trykke på et ondsinnet vedlegg eller lenke til skadelig kode. Formålet kan også være å lure personer til å gi fra seg sensitiv informasjon eller betalingsopplysninger. Disse angrepene er ofte målrettet eller skreddersydd mot enkeltpersoner som f.eks. ledere eller personer med ansvar for økonomi og sensitiv informasjon (NSR, 2018). Et annet utbredt virkemiddel er skanning, etterfulgt av

utnyttelse av sårbarheter i systemer. Dette er en fremgangsmåte som ikke er målrettet på samme måte som phishing, men som heller rammer virksomheter med kjente sårbarheter. Dette er et angrep som foregår gjennom at en skanner etter sårbare versjoner av programvare i et nettverk. Hvis bedrifter ikke har oppdatert programvare, kan dette gi angripere en åpning til å komme inn i bedriftens nettverk (NSR 2018).

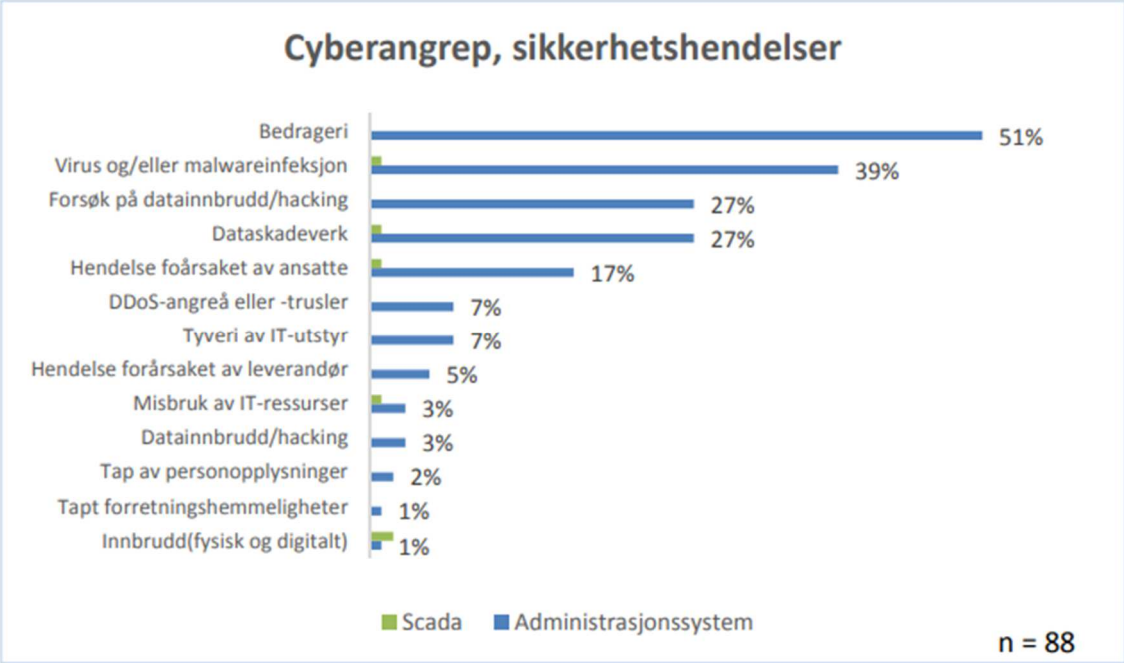
Trusler om, og gjennomføring av DDoS-angrep (Distributed Denial of Service), eller et såkalt tjenestenektangrep forekommer også. Dette er et angrep der det forsøkes å hindre at brukere får tilgang til en tjeneste eller informasjon, gjennom å f.eks. oversvømme et nettsted med trafikk (Nettvett, 2019). Norske virksomheter kan trues med krav om å betale hackerne for å hindre påståtte angrep. Det gjennomføres også andre utpressingsangrep i form av løspengevirus (ransomware) der skadevare krypterer filer på den infiserte datamaskinen slik at dem blir utilgjengelig for eieren. I dette tilfellet blir offeret bedt om å betale penger for å få tilbake tilgangen til filene. (Nettvett, 2019; NSM, 2018)

Selv om cyberangrep ofte utnytter tekniske sårbarheter i programvare, ser en ofte at kriminelle forsøker å manipulere mennesker. Sosial manipulering (*social engineering)* går ut på å skaffe seg tilgang gjennom å lure noen til å gi fra seg f.eks. passord eller sensitiv informasjon (NOU,2015). Dersom mennesker ikke er bevisste nok på hva som utgjør en sikkerhetsrisiko, kan de la seg lure til å begå feil som forårsaker at uvedkommende får tilgang til sensitiv informasjon. Det er dermed ikke tilstrekkelig med bare sikker teknologi dersom mennesker på innsiden av organisasjonen gir fra seg tilgang til uvedkommende. Cybersikkerhet er dermed høyst avhengig av organisasjonen og menneskene som jobber i den (Line & Tøndel 2012).

2.3 Cybersikkerhet i kraftsektoren

Den største sikkerhetsutfordringen i kraftforsyningen har tradisjonelt vært slitasje og nedetid som følge av værforhold (NOU, 2015). Etter utviklingen av digitaliseringen opplever kraftsektoren i likhet med de fleste andre virksomhetstyper at cyberangrep blir en større del av trusselbildet. I PSTs *Trusselvurdering 2019* (2019) forventes det at fremmed etterretningsvirksomhet vil forsøke å erverve inngående kjennskap til kritisk infrastruktur (PST, 2019). Norsk kraft er viktig for stabiliteten i kraftmarkedet i Norden og deler av Europa, og en må derfor se trusselen mot norsk kraftforsyning i en større europeisk sammenheng (NVE, 2017b).

Cybertruslene som kraftsektoren står ovenfor er varierte, og trusselaktørene kan være alt fra profesjonelle aktører og enslige amatør hackere, til utro ansatte på innsiden av virksomheten (NOU, 2015; NVE, 2017a). Ifølge tall fra NVE (2017a) rapporterte 51% av virksomhetene at de hadde opplevd bedrageri rettet mot sine administrasjonssystemer det siste året. Dette dreier seg hovedsakelig om svindelforsøk via epost. 39% opplevde å få infisert virus i IKT-systemene. Andre uønskete hendelser omfatter blant annet skadevarer i form av løspengevirus, som har som hensikt å redusere tilgjengeligheten til data. **Figur 2** viser oversikt over hvilke cyberangrep og øvrige uønskete informasjonssikkerhetshendelser virksomhetene har vært utsatt for siste 12 måneder.



Figur 2 Informasjonssikkerhetshendelser siste 12 måneder (NVE, 2017a, s.13).

Som det fremkommer av **Figur 2**, så er majoriteten av cyberangrepene rettet mot virksomhetenes administrasjonssystem, mens en mindre andel er rettet mot SCADA-systemene. Med tanke på et mulig brudd i strømforsyningen er angrepene mot SCADA-systemene de mest bekymringsfulle. Angrep mot administrasjonssystemene kan derimot utgjøre en betydelig risiko for øvrig informasjonssikkerhet i virksomhetene, samt utnyttes til å skaffe informasjon om hvordan en kan angripe SCADA-systemene slik angriperne i Ukraina gjorde (Jaatum et al., 2017).

NVE spurte virksomhetene i 2017 om hva som var den mest alvorlige IKT-sikkerhetshendelsen og hvilke konsekvenser den fikk. Dataskadeverk som løspengevirus, tett etterfulgt av bedrageri var de mest utbredte typene av alvorlige uønskete hendelser. I de fleste tilfellene medførte ikke hendelsen noen konsekvenser, men i 12% av tilfellene medførte hendelsene driftsavbrudd. Noen opplevde også økonomiske tap og mediedekning (NVE, 2017a). Av medvirkende faktorer til at hendelsen oppstod svarer 42% av virksomhetene at de ikke vet hvorfor hendelsen oppstod. De mest hyppig siterte årsakene er menneskelig feil og manglende sikkerhetsbevissthet. Samme undersøkelse viser at mer enn en av fire virksomheter svarer at de enten ikke har, eller ikke vet om de har et overordnet rammeverk for styring av informasjonssikkerhet. Selv om påliteligheten i den norske kraftsektoren er veldig god, er det mye som tyder på at det eksisterer et forbedringspotensial for håndteringen av cybersikkerhet i bransjen.

3. Teori

I dette kapittelet vil studiens teoretiske utgangspunkt presenteres. I kapittel 2 ble det argumentert for at cybersikkerhet omfatter både safety og security. Litteraturen som har formet det teoretiske rammeverket for studien er i all hovedsak teori innenfor safety-domenet, altså teori om ikke-tilsiktede ulykker. Dette er teoretiske bidrag som også kan anvendes innenfor cybersikkerhet, ettersom både safety og security omhandler å beskytte verdier mot ulike trusler gjennom å redusere sårbarhet. Nøkkelen til dette er god risikostyring. Derfor vil det først presenteres teori om risikostyring med fokus på ulike typer barrierer.

Et nettselskap er ansvarlig for å drifte strømnettet og sørge for at strømmen fra kraftleverandøren blir transportert til sluttbrukeren. Dette er virksomheter som består av et samspill mellom mennesker, teknologi og organisasjon. Det kan derfor sies å være et sosioteknisk-system som kan analyseres innenfor et MTO-perspektiv. Ettersom studien fokuserer på ikke-tekniske barrierer vil utdypingen av MTO-perspektivet fokusere på de menneskelige og organisatoriske forholdene. For å forklare den menneskelige faktoren vil bidrag fra Dekker (2006) og Reason (1997) presenteres. For å vise hvordan menneskelige aktive feil henger sammen med organisatoriske forhold vil Reasons teori om organisatoriske ulykker legges frem.

Til slutt vil Weick Sutcliffe & Obstfeld (1999) sitt begrep om kollektiv bevissthet (mindfulness) presenteres. Kollektiv bevissthet er en tilnærming innenfor fagfeltet om høypålitelige

organisasjoner (HRO). Dette perspektivet benyttes for å ytterligere forklare hvordan organisatoriske forhold påvirker påliteligheten på barrierene i nettselskapene.

3.1 Risikostyring

Risikostyring kan defineres som «*alle tiltak og aktiviteter som gjøres for å styre risiko*» (Aven, 2007, s.13). Det finnes utallige definisjoner og tilnærminger til risikobegrepet, men i denne studien defineres risiko som *«en kombinasjon av mulige konsekvenser (utfall) og tilhørende usikkerhet»* (Aven, 2007, s.41). Det er vanlig å operasjonalisere usikkerhet til et uttrykk for hvor sannsynlig det er at en hendelse vi har identifisert kan inntreffe. Dette innebærer naturligvis en forenkling av virkeligheten, ettersom det alltid vil foreligge en usikkerhet utover det vi klarer å fange opp og sette ord på i vår sannsynlighetsbeskrivelse (Lunde, 2014). Beskrivelse av sannsynlighet kan være en vesentlig utfordring ovenfor intenderte hendelser, ettersom en i mange tilfeller vil mangle kunnskap om aktørers planer om å utføre en ondsinnet handling (Engen et al., 2016, Jore & Njå, 2010). Mange av hendelsene en står ovenfor vil dermed være ukjente. Innenfor enkelte typer cyberkriminalitet vil imidlertid flere av hendelsene være kjente ettersom det er mye erfaringsdata å bygge risikovurderinger på (Jore & Egeli, 2015 i Engen et al., 2016).

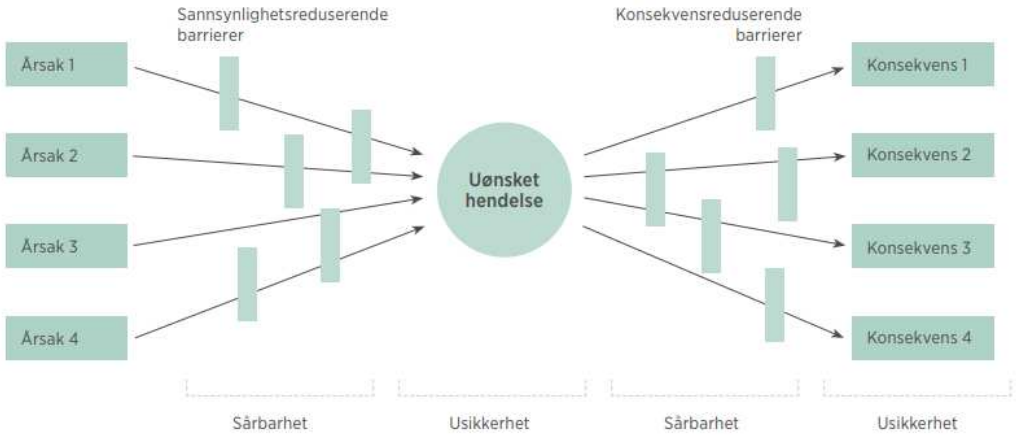
Alle virksomheter som skaper verdier må akseptere at de også forholder seg til risiko. Det blir derfor viktig å ha en balanse mellom det å skape verdier, og å unngå ulykker, skader og tap (Aven, 2007). Risikostyring er dermed ikke en ensidig prosess som bare handler om å redusere risiko. Risikostyring handler både om å få innsikt i risikoforhold, grad av styrbarhet av risikoen, samt metoder, prosesser og strategier for å kartlegge og styre den (Aven, 2007, Lunde, 2014). Hvis en virksomhet skal redusere risiko, er det nødvendig å iverksette tiltak som enten reduserer sannsynligheten for at uønskete hendelsene inntreffer, eller tiltak som er egnet til å redusere konsekvensene av de uønskete hendelsene (Lunde, 2014).

Litteratur om risikostyring i møte med intenderte hendelser henviser ofte til risikovurdering gjennom trefaktormodellen (Engen et al., 2016). Risikovurderingen sammensettes på bakgrunn av kunnskap om verdier, trusler og sårbarhet. Verdier utgjør det som en ønsker å beskytte, som for eksempel strømforsyningen eller sensitiv informasjon. Trusler kan være ulike ondsinnete handlinger rettet mot verdiene som f.eks. løspengevirus som medfører at sensitiv informasjon krypteres. For å vurdere truslene henvises det ofte til trusselaktørenes intensjon og kapasitet. I henhold til potensielle cyberangrep avgjøres trusselen om hvorvidt noen har både intensjon og

kapasitet til å gjennomføre et cyberangrep. Sårbarheten må sees i sammenheng med hvilken evne organisasjonen har til å forsvare verdiene sine mot ulike trusler (Engen, et al., 2016).

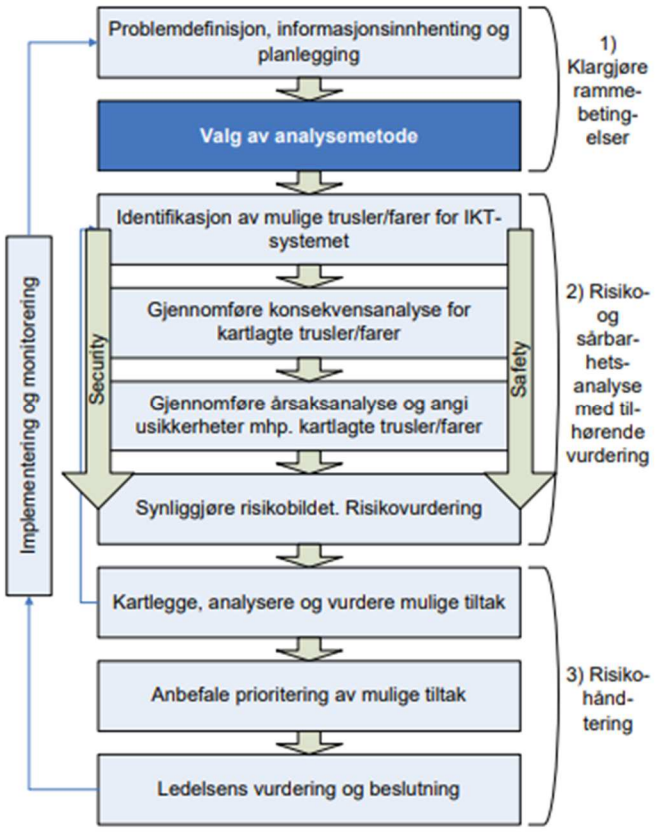
En sentral del av risikostyringsprosessen er å gjennomføre risiko- og sårbarhetsanalyser (ROS-analyser) (Lunde, 2014). En ROS-analyse er en analyse av risiko. ROS-analysen omfatter identifisering av initierende hendelser, årsaksanalyse, konsekvensanalyse og risikobeskrivelse (Aven, 2007). Hensikten er å gi innsikt om risiko knyttet til en aktivitet eller et system, og analysen skal fungere som et underlag for beslutninger om hvilke løsninger og tiltak som skal iverksettes.

Ettersom sårbarhet er et aspekt av risiko, er sårbarhetsanalyse en del av risikoanalysen (Aven, 2007). Sårbarhet kan defineres som *«et uttrykk for de problemer et system vil få med å fungere når det utsettes for en uønsket hendelse, samt de problemer systemet får med å gjenoppta sin virksomhet etter at hendelsen har inntruffet»* (Sårbarhetsutvalget, 2000 i Aven, 2007). De fleste produksjonssystemer og organisasjoner er utsatt for ekstern og intern påvirkning, og noen systemer bringes lettere i ubalanse ettersom de mangler interne korrigeringstiltak for å rette opp i forstyrrelsene (Karlsen, 2010). En måte å uttrykke sårbarhet på er gjennom sannsynlighet for at en ønsket funksjon (f.eks. strømforsyning) ikke ivaretas gitt en initierende hendelse (Aven, 2007). I stor grad er sårbarhet selvforskyldt, og det går an å påvirke sårbarheten gjennom tiltak som reduserer den. Ofte benyttes begrepet robusthet som det motsatte av sårbarhet (Engen, et al., 2016). En måte å oppnå robusthet er å danne og vedlikeholde barrierer. Dersom en har gode barrierer, har man generelt liten sårbarhet (Aven, 2007). **Modell 1** illustrerer et sløyfediagram som presenterer et risikobilde. Sløyfediagrammet viser sammenhengen mellom uønskete hendelser, barrierer og konsekvenser for en identifisert uønsket hendelse.



Modell 1 Eksempel på sløyfediagram (DSB, 2014, s. 26)

Den venstre siden av sløyfediagrammet viser mulige årsaker, sårbarheter, og risikoreduserende tiltak. Den høyre siden viser de konsekvensreduserende tiltakene som er iverksatt, og konsekvenser som kan oppstå som resultat av den uønskete hendelsen. De risikoreduserende og konsekvensreduserende tiltakene kan sees på som barrierer. Generelt vil en vurdering av sårbarheten omfatte vurderinger av de ulike barrierene i henhold til effektivitet, kapasitet og pålitelighet (Aven, 2007). **Modell 2** viser en standard risikostyringsprosess av et IKT-system (Sivertsen, 2007).



Modell 2 Risikostyringsprosess (Sivertsen, 2007, s. 12).

Modellen illustrerer at risikostyringsprosessen kan deles opp i tre hovedfaser. I den første fasen klargjøres rammebetingelsene gjennom problemdefinisjon og valg av analysemetode. Deretter må risikobildet beskrives gjennom ROS-analyser. Som vi ser av figuren inkluderer dette safety- og security-relatert risiko. På bakgrunn av risikovurderingene planlegges og vurderes ulike tiltak som kan benyttes i den tredje hovedfasen: risikohåndtering. Analysene fungerer som et

beslutningsunderlag for ledelsen som må vurdere hvilke tiltak som skal iverksettes. Disse tiltakene kan anses som barrierer. Dette er en kontinuerlig prosess, ettersom en må monitorere ytelsen av tiltakene og overvåke effekten på risikoen (Sivertsen, 2007).

3.1.1 Barrierer

I risikostyringen er barrierene viktige styringsvariabler. Dette gjelder både i prosjekteringsfasen hvor barrierene velges, dimensjoneres og bygges inn, og i driftsfasen hvor barrierene vedlikeholdes og forbedres. Endring i ytelsesnivået til en barriere endrer risikonivået, og overvåkning av slike endringer vil være en viktig del av sikkerhetsarbeidet (Aven, Boyesen, Olsen, Njå & Sandve, 2004). Det er derfor viktig å forstå barrierer for å forstå forebygging av uønskete hendelser. Det faktum at en uønsket hendelse har skjedd betyr at en eller flere barrierer har feilet, ikke vært til stede eller ikke utført sin funksjon (Hollnagel, 1999).

Barrierebegrepet ble introdusert i Gibsons energimodell i 1961. Haddon (1970) videreutviklet barrierebegrepet med sine 10 strategier for å hindre ulykker (Haddon, 1970 i Rosness et al., 2002). Det finnes utallige definisjoner på hva en barriere er, men det er ingen presis samlende definisjon (Rosness et al., 2002). Felles for de fleste definisjonene er at de referer til en farekilde som skal forsvares mot, mens forskjellene er om hvorvidt barrierebegrepet skal begrenses til fysiske tiltak, eller om det også omfatter administrative tiltak og menneskelig intervensjon (Rosness et al., 2002). Hollnagel (1999) definerer en barriere som noe som hindrer en uønsket hendelse fra å skje, eller som reduserer konsekvensene av en uønsket hendelse (Hollnagel, 1999). Begrepet barriere kan gi assosiasjoner til fysiske stengsler. Det er imidlertid mer nyttig å forstå begrepet barriere i et funksjonelt perspektiv, der barrierer ansees som enhver sikkerhetsfunksjon som har som mål å forhindre ulykker inklusivt prosedyrer og opplæring. (Rosness et al., 2002). Denne forståelsen av barrierer er derfor lagt til grunn i denne studien.

Barrierer er et viktig virkemiddel for å skape en feiltoleranse, slik at menneskelige feilhandlinger og teknisk svikt ikke umiddelbart fører til ulykker, eller at eventuelle konsekvenser blir mest mulig redusert (Rosness et al., 2002).

Reason (1997) skiller mellom harde og myke barrierer. Harde barrierer inkluderer tekniske og automatiserte sikkerhetsfunksjoner som fysiske barrierer, alarmer, låser og personlig verneutstyr (Reason, 1997). Innen cybersikkerhet kan en anse antivirus, brannmurer, og kryptering som harde barrierer. Myke barrierer omfatter en kombinasjon av mennesker og papirer. Reason eksemplifiserer de myke barrierene gjennom lovgivning, tilsyn, regler og

prosedyrer, trening, opplæring, øvelser, administrativ kontroll, sertifisering og personell i den «skarpe enden» (Reason, 1997).

Hollnagel (2008) grupperer barrierer som materielle (fysiske), funksjonelle, symbolske, og immaterielle. De materielle barrierene omfatter det som Reason (1997) kategoriserer som harde barrierer. En funksjonell barriere har en eller flere forutsetninger som må imøtekommes før den kan aktiveres. Enkelte typer funksjonelle barrierer trenger at et menneske aktiverer barrieren, mens andre er automatiserte og består bare av teknologi (Hollnagel, 2008). Innenfor cybersikkerhet kan en si at en brannmur er en materiell barriere, mens pålogging via tofaktorautentisering[1] er en funksjonell barriere. De symbolske barrierene virker indirekte gjennom at meningen med dem tolkes av noen (Hollnagel, 2008). En sikkerhetsprosedyre er et eksempel på en symbolsk barriere. De immaterielle barrierene er ikke fysisk til stede i de situasjonene der de skal anvendes, men avhenger fullstendig av kunnskapen brukeren har for å oppnå sin funksjon. Dette er barrierer som også ofte omtales synonymt med organisatoriske barrierer, da de er barrierer som organisasjonen har pålagt systemet, men som ikke er fysisk, funksjonelt eller symbolsk til stede i systemet. Noen eksempler på organisatoriske barrierer er: lover og regler, etiske normer og sosialt press (Hollnagel, 2008).

For at barrierer skal være effektive må som regel de ulike kategoriene av barrierer kombineres (Hollnagel, 2008). Hollnagel (2008) hevder at symbolske og immaterielle barrierer ofte må kombineres med fysiske og funksjonelle barrierer for å fungere. Immaterielle og symbolske barrierene kan ikke alene utøve en sikkerhetsfunksjon, ettersom de er avhengig av at et menneske må tolke og forstå hvordan barrieren i praksis skal iverksettes gjennom deres adferd. De ansattes adferd iverksetter dermed barrierens funksjon. På bakgrunn av dette hevder Hollnagel at de immaterielle barrierene er minst effektive, ettersom de baserer seg fullstendig på at brukerne bestemmer seg for at barrieren skal fungere. Tilsvarende er symbolske barrierer også ineffektive, ettersom brukerne kan bestemme seg for å ignorere dem. For å illustrere symbolske barrierers ineffektivitet, henviser Hollnagel til advarslene på sigarettpakker (Hollnagel, 2008).

En måte å kombinere ulike former for barrierer, er strategien «forsvar-i-dybden» (Reason, 1997). Reason (1997) hevder at alle barrierer er designet for å oppfylle en eller flere av følgende funksjoner:

[1] Tofaktorautentisering betyr at du i tillegg til passord må angi en engangskode hver gang du logger inn på en tjeneste.

1. Å skape forståelse for, og bevissthet om en trussel.
2. Å gi en klar veiledning om hvordan operere sikkert.
3. Å fungere som alarm, eller gi advarsel når en trussel nærmer seg
4. Å trygt gjenopprette systemet etter en unormal situasjon.
5. Å legge inn sikkerhetsbarrierer mellom en trussel og mulige tap
6. Å kontrollere og eliminere trusler dersom de skulle unnslippe barrierene
7. Å gi mulighet for å rømme og reddes, dersom alle andre barrierer mislykkes.

Forsvar-i-dybden er en utbredt strategi for organisering av barrierer. Den grunnleggende tanken bak forsvar-i-dybden er at ingen enkelt menneskelig- eller teknisk feil skal kunne lede til ulykker. Forsvar-i-dybden har to formål: (1) forebygge ulykker, og (2) begrense konsekvensene dersom en ulykke inntreffer (Rosness et al., 2002). Dette innebærer at en etablererer suksessive lag med uavhengige barrierer, slik at dersom en barriere svikter, vil en annen barriere demme opp for den uønskete hendelsen**.**

3.2 MTO – Mennesker, teknologi og organisasjon

MTO-perspektivet har blitt en stadig større del av moderne sikkerhetsarbeid. MTO-perspektivet handler om å studere samspillet mellom *menneskelige(M), teknologiske(T)* og *organisatoriske(O)* faktorer. På starten av 90-tallet fikk MTO-perspektivet fotfeste fordi en kunne observere at ulykker generelt oppstod i samspillet mellom teknologien, mennesket og organisasjonen (Bento, 2001, Rollenhagen 1997). MTO-problemer kan analyseres i et systemisk perspektiv. Dette innebærer en helhetlig tilnærming til relasjonene mellom delsystemene, istedenfor å fokusere på hvert delsystem alene (Rollenhagen, 1997). Bento (2001) presenterer flere faktorer som fører til at MTO-problemer forekommer. Han hevder at en ikke tar hensyn til menneskets begrensninger og menneskelig adferd når ny teknologi introduseres. Videre bemerker Bento at det i etterkant av en uønsket hendelse er en tendens til å skylde på teknisk svikt, uten at det tas hensyn til hvilke organisatoriske betingelser som påvirker at teknologi svikter. Eksempler på dette kan være svak sikkerhetskultur, mangelfullt system for vedlikehold og at ledelsens retningslinjer og målsettinger ikke er godt nok definert, formidlet, eller forstått (Bento, 2001).

Albrechtsen & Hovden (2011) hevder at god cybersikkerhet oppnås gjennom samspillet mellom mennesker, teknologi og organisasjon og at cybersikkerhet[2] må forstås innenfor et sosioteknisk-system. Teknologi er selvsagt basisen for cybersikkerhet, men teknologien må i imøtekomme menneskelige, organisatoriske og samfunnsmessige behov for å være suksessfull. Et sosioteknisk cybersikkerhetssystem består av et samspill av blant annet: tekniske løsninger, regler, prosedyrer og instrukser for individuell og organisatorisk adferd, rollen og ansvaret til IT-sikkerhetspersonell, kollektive normer og verdier, og interaksjonen mellom individer og grupper. Disse faktorene produserer en rekke tekniske og ikke-tekniske elementer som til sammen utgjør cybersikkerheten. Cybersikkerhet er dermed en tverrfaglig disiplin, og bør inkludere ikke-tekniske elementer i tillegg til de tekniske (Albrechtsen & Hovden, 2011).

3.2.1 Den menneskelige faktoren

«*We cannot change the human condition, but we can change the conditions under which people work*» Reason (1997, s. 15)

Det er mennesker som både lager og designer teknologi i tillegg til å styre, vedlikeholde og beskytte den. Det er dermed helt naturlig at menneskers bidrag vil være sentrale både i å forårsake og forhindre ulykker (Reason, 1997). Mennesker er alltid en del av MTO-problem, men mennesker er ikke alltid den eneste kilden til problemet (Bento, 2001). Menneskelig feil blir ofte trukket frem som en forklaring på hvorfor ulykker oppstår. En menneskelig feil kan defineres som «*the failure of planned actions to achieve their desired ends- without the intervention of some unforeseeable event*» (Reason, 1997, s. 71).

Enkelte påstår at menneskelig feil kan forklare så mye som 80-90% av ulykker. Reason (1997) mener at dette antageligvis er et godt estimat med tanke på hvor involvert mennesker er i risikofylt teknologi, men at slike estimater forteller lite om hvorfor ulykker egentlig oppstår. En menneskelig feil er nemlig ikke noe som forklarer hvorfor ulykker oppstår, men noe som trenger en forklaring (Reason, 1997). Sidney Dekker (2006) nyanserer imidlertid menneskelige feil som årsak til at ulykker oppstår. Bak menneskelige feilhandlinger er det som regel en rekke andre forhold som har påvirket mennesket i den skarpe enden til å begå feilen. Ofte viser det seg at en handling som var feil, ga mening da den ble gjort, basert på handlerens informasjon på daværende tidspunkt (Dekker, 2006).

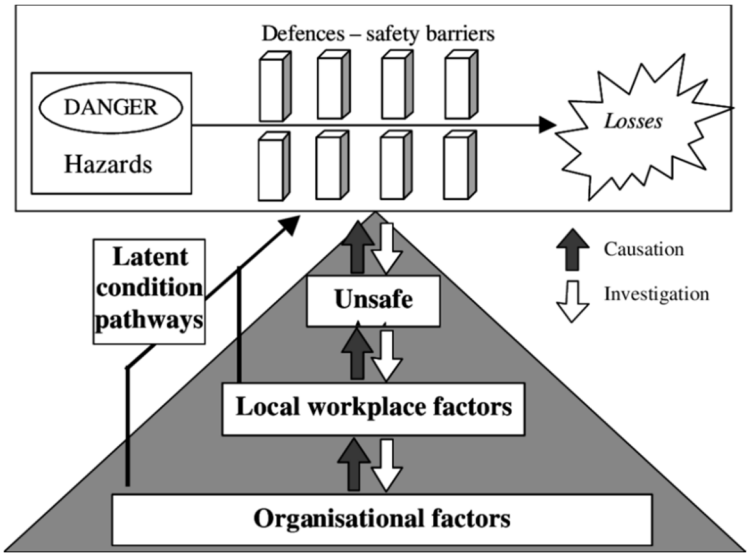
[2] Her må det bemerkes at Albrechtsen & Hovden (2011) bruker begrepet informasjonssikkerhet. Gjennomgangen av cybersikkerhetsbegrepet i kapittel 2 viser at disse begrepene i praksis kan brukes om hverandre.

Sidney Dekker skiller mellom «The Old View» og «The New View» av menneskelig feil. «The Old View» representerer et syn som ser på menneskelige feil som en årsak i seg selv til at uønskede hendelser oppstår. Komplekse systemer ville vært trygge så lenge det ikke var for uaktsom adferd av enkelte ansatte. Ansatte som gjør feil og utøver uaktsom adferd blir omtalt som «Bad Apples» (Dekker, 2006). «The Old View» hevder at feil oppstår som uforventete overraskelser som i utgangspunktet ikke hører hjemme i systemet. Feil introduseres i systemet av upålitelige mennesker, og man må fjerne disse feilene, eller menneskene som utøver dem for å eliminere farer (Dekker, 2006).

«The New View» ser derimot på feil som et symptom på dypere svikt i systemet. Dekker introduserer «*The Local Rationality Principle*» som handler om at folk stort sett gjør fornuftige valg gitt kunnskapen som lå til grunn på det tidspunktet feilen ble begått. De aller færreste ansatte velger å gjøre feil intensjonelt. I det nye synet på menneskelige feil ser man heller på karakteristikker ved selve systemet som forklaringer på hvorfor mennesker gjør feil. Det er en rekke forhold som påvirker sannsynligheten for feilhandlinger. Dette kan eksempelvis være fysiske forhold med arbeidsplassen, tids- og arbeidspress, opplæring og sikkerhetskultur (Bento, 2001 Dekker, 2006). En organisasjon har som regel mange andre mål enn bare sikkerhet, og på grunn av konflikterende målsetninger og press kan mennesker begå feilhandlinger. Ofte vil ansatte velge å ta snarveier og slakke på sikkerhetskravene av hensyn til f.eks. produktivitet og effektivitet (Dekker, 2006, Rasmussen, 1997).

3.2.2 Organisatoriske ulykker

Reason (1997) introduserte begrepet organisatoriske ulykker, som er store ulykker som har sammensatte årsaksforhold og involverer mange mennesker på ulikt nivå i en organisasjon. Reason skiller mellom organisatoriske og individuelle ulykker, der førstnevnte omfatter storulykker som f.eks. flyulykker og skipsforlis, mens sistnevnte er ulykker som bare berører enkeltpersoner, (Reason, 1997). I denne studien kan et større hackerangrep som f.eks. angrepet som rammet Ukraina anses som en organisatorisk ulykke. **Modell 3** viser at organisatoriske ulykker er sammensatt av en rekke årsaker.



Modell 3 Organisatoriske ulykker (Reason, 1997, s. 17).

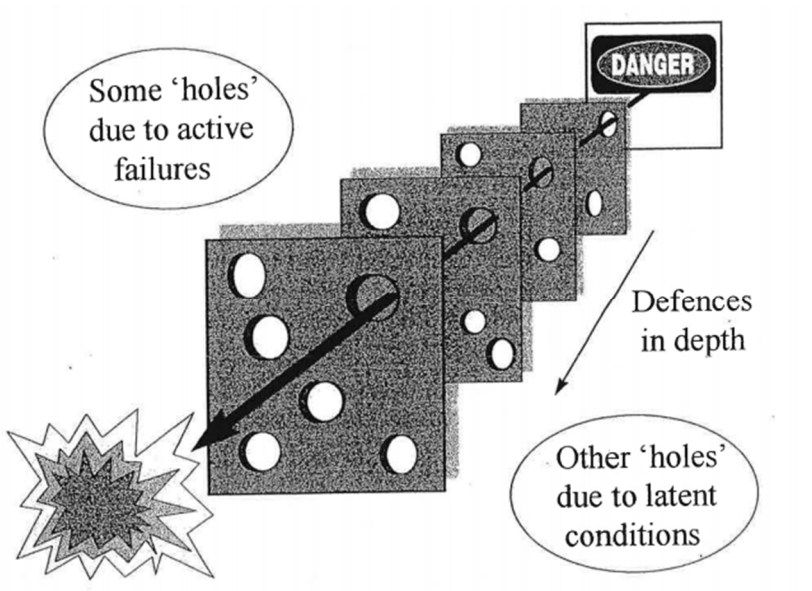
Modellen er sammensatt av tre nivå: de organisatoriske faktorene, de lokale faktorene, og utrygge handlinger (Reason, 1997). Ulykker har ofte sitt opphav i de organisatoriske forholdene, som igjen vil påvirkes av lokale faktorer. En ulykke utløses ofte av utrygge handlinger, men disse er ofte påvirket av lokale og organisatoriske forhold (Bento, 2001; Dekker, 2006).

Organisasjonskultur er ifølge Reason (1997) verdier og oppfatninger som menneskene i systemet har til felles. Disse bestemmer hva som er viktig for organisasjonen og produserer atferdsnormer. Dette kan vise seg i organisatoriske forhold som f.eks. ved prioritering av ressurser, administrasjon og budsjettering. Dette er faktorer som vil påvirke holdninger, normer, atferdsmønstre og kulturen for hvordan en organisasjon driver sitt sikkerhetsarbeid. Lokale faktorer kan f.eks. være tidspress, utilstrekkelig utstyr, underbemanning, dårlig kommunikasjon, og mangelfulle prosedyrer. Disse faktorene vil sammen med menneskelige utrygge handlinger skape feil, som gjør at en uønsket hendelse inntreffer (Rasmussen 1997; Reason, 1997). Organisatoriske forhold legger også føringer for sikkerhetskulturen. Sikkerhetskultur kan defineres som:

> *«… et produkt av individuelle- og gruppe verdier, holdninger, kompetanse og atferdsmønstre som viser forpliktelse, og dyktigheten til en organisasjons helse- og sikkerhetsprogrammer. Organisasjoner med en positiv sikkerhetskultur karakteriseres ved kommunikasjon basert på gjensidig tillit, felles oppfatninger om viktigheten av sikkerhet og med tiltro til organisasjonens sikkerhetsmål.»* (Reason, 1997, s. 194)

I Reasons teori om organisatoriske ulykker benytter han begrepene «aktive feil» og «latente forhold». Aktive feil beskriver handlinger som blir begått av personell og operatører i den skarpe enden av systemet. Dette er handlinger som har direkte negative konsekvenser for sikkerheten i systemet. Latente forhold har sitt opphav i strategiske beslutninger fra ledelsen, myndighetene, leverandører, og ledere i organisasjonen. Disse strategiske beslutningene bidrar til å skape en kultur og rammebetingelser som påvirker sannsynligheten for aktive feil. De latente forholdene kan være dårlig design, manglende administrativ kontroll, uhåndterlige prosedyrer, mangelfull opplæring og trening, utilstrekkelige verktøy og teknologi. Dette er forhold som kan være til stede over flere år, før det kombinert med en aktiv feil fører til en organisatorisk ulykke (Reason, 1997).

En aktiv feil kan medføre en spesifikk type ulykke, mens latente forhold kan bidra til en rekke forskjellige typer ulykker. Latente forhold er til stede i alle typer system, og er en uunngåelig del av en organisasjons liv (Reason, 1997). **Modell 4** viser sveitserostmodellen som illustrerer hvordan en organisasjons sikkerhetsbarrierer gjennomtrenges. Barrierene har hull som kan skyldes både aktive feil og latente forhold, og når alle gjennomtrenges inntreffer ulykken (Reason, 1997).



Modell 4 Sveitserostmodellen (Reason, 1997, s. 12).

3.3 HRO og kollektiv bevissthet

High Reliability Organizations (HRO) er organisasjoner som lykkes i å unngå alvorlige ulykker i komplekse høyteknologiske system (Weick et al., 1999). HRO-perspektivet er et perspektiv innen organisatorisk sikkerhetsstyring som har blitt utviklet gjennom å studere organisasjoner som har vist evne til å håndtere kompleks og krevende teknologi uten store ulykker. HRO-teoriene oppstod delvis som et motsvar til Charles Perrow (1984) sin bok *Normal Accidents*, som hevder at organisatoriske ulykker i komplekse og tett koplete høyteknologiske system er uunngåelig (Weick et al., 1999). Det er en rekke forskjellige teoretikere som har bidratt med å utvikle kjennetegn for hva som utgjør en HRO (Aven & Krohn, 2013; LaPorte & Consolini, 1991; Rochlin, 1993 Weick et al., 1999). Selv om de ulike teoretikerne operer med noe ulikt fokusområde, og innfallsvinkler til sikkerhetsstyring, eksisterer det et kjernebudskap om at risiko i organisasjoner kan styres (Aven et al., 2004). Dette innebærer et gjennomgående fokus på sikkerhetsstyring, og troen på god risikostyring. HRO-perspektivet kan anses som en normativ tilnærming til sikkerhetsstyring som innebærer at det er et ideal å strekke seg etter, men at en i praksis bare vil delvis kunne oppfylle de ulike kjennetegnene (Aven et al., 2004).

En sentral tilnærming innenfor HRO-perspektivet er begrepet om kollektiv bevissthet (mindfulness) som ble introdusert av Karl Weick (Weick & Sutcliffe, 2007; Weick et al., 1999). Begrepet kollektiv bevissthet er et forsøk på å operasjonalisere sentrale karakteristikker som identifiseres i høypålitelige organisasjoner. Dette er karakteristikker som har en avgjørende betydning for hvorvidt en organisasjon vil være i stand til å kontinuerlig opprettholde et godt sikkerhetsnivå i et dynamisk miljø (Aven & Krohn, 2013). Weick & Sutcliffe (2007) argumenterer for at dette oppnås gjennom det som beskrives som den kollektive bevisstheten, som gjør at organisasjonen er i stand til å kontinuerlig overvåke kjente og ukjente farer, og håndtere disse etter hvert som de oppstår. Kollektiv bevissthet handler om å anerkjenne at uventede hendelser kan oppstå hvor som helst i organisasjonen. Denne bevisstheten hevder Weick et al., (1999) at en organisasjon kan oppnå gjennom fem kognitive prosesser. Aven & Krohn (2013) argumenterer for at disse fem kognitive prosessene kan brukes innenfor risikostyring. De fem kognitive prosessene er:

1. Opptatt av feil og svikt (Preoccupation with failure)

En HRO er konstant bevisst på at det til enhver tid kan oppstå overraskelser og feil. En spesiell karakteristikk ved en HRO er at det sjeldent forekommer feil og svikt, samtidig som en

bestandig er opptatt av å avdekke feil. En HRO er altså opptatt av noe de sjeldent ser, og når feil forekommer blir de grundig analysert (Weick et al., 1999). En HRO oppfordrer til, og belønner rapportering av feil, og den håndterer fortløpende det som rapporteres inn for å ta lærdom av disse feilene. Rapporteringssystemet bør være effektivt og brukervennlig (Reason, 1997). Reason (1997) hevder en rapporterende kultur klarer å kartlegge uønskete hendelser, og nesten-hendelser dersom de ansatte har tillit til rapporteringssystemet, og ser nytten av å rapportere. Hvis en antar at feil er en viktig forutsetning for læring er det vanskelig for en HRO å lære. En HRO må derfor utvide læringsmulighetene sine ved å analysere nesten-hendelser. En HRO lokaliserer ikke feil, men generaliserer istedenfor de feilene de finner, som et symptom på dypere trøbbel i systemet. Akkumuleringen av små hendelser øker sannsynligheten for at en stor hendelse kan oppstå (Weick et al., 1999). Dersom menneskene i organisasjonen er oppmerksomme og ser etter små feil og avvik, kan en forhindre at større hendelser får utvikle seg. Det samme gjelder nesten-ulykker. Selv om en hendelse ble avverget, bør det behandles som et signal på at systemet ikke er trygt ettersom det nesten oppstod en uønsket hendelse, eller større ulykke (Weick & Sutcliffe, 2007).

2. Motstand mot forenkling av tolkninger (Reluctance to simplify interpretations)

Personell i alle organisasjoner håndterer komplekse oppgaver gjennom å gjøre forenklinger i sine tolkninger av gitte situasjoner. Disse forenklete tolkningene kan beskrives som en form for verdensbilde eller tankesett som gjør at en kan ignorere informasjon og fortsette å arbeide som en alltid har gjort (Turner, 1978 i Weick 1999). Dette er en vanlig karakteristikk i de fleste organisasjoner. Disse forenklingene er potensielt farlige for en HRO, ettersom de begrenser forholdsreglene personell forholder seg til, og dermed ignorerer potensielle uønskete hendelser. I en HRO er det derfor motstand mot denne type forenklinger av virkeligheten, ettersom dette kan medføre at viktig informasjon ignoreres. I en HRO eksisterer det en form for skepsis som medfører at operasjoner, rutiner og prosedyrer alltid utfordres og vurderes. Overforenklete rutiner og standardiserte prosedyrer kan være nyttig for å samle kunnskap, men kan også være en trussel for sikkerheten. Gjennom å forholde seg kritisk til egen praksis oppstår det en form for redundans, ettersom alle rutiner og operasjoner møtes med skepsis. Utfordringen en HRO står ovenfor er å vurdere hvilken informasjon som kan ignoreres, og hva som må tas hensyn til (Weick et al., 1999).

3.Operasjonssensitivitet/årvåkenhet (Sensitivity to operations)

Sensitivitet til pågående operasjoner handler om å sanse hva som foregår og handle deretter (Aven & Krohn, 2013). Dette handler om å være årvåken, som er et begrep som kan relateres til begrepet situasjonsforståelse. Denne situasjonsforståelsen oppstår gjennom å være oppmerksom på hva som skjer rundt en, og å forstå hva informasjonen betyr nå og i fremtiden. Kollektiv bevissthet innebærer mer enn situasjonsforståelse ettersom kollektiv bevissthet handler om å se det store bildet som inkluderer eksisterende forventinger, kontinuerlig tilpasning å forestille seg fremtidige tilstander av situasjonen. Ettersom HRO innebærer kompleks teknologi som opererer i et komplekst miljø er en avhengig av deling av informasjon og tolkning mellom enkeltpersoner. En effektiv HRO anerkjenner de begrensete kognitive ressursene til enkeltindividet. Å oppnå årvåkenhet og operasjonssensitivitet er dermed ofte en delt oppnåelse mellom flere personer (Weick et al., 1999).

Nøkkelen til å oppnå operasjonell sensitivitet er å ha oppmerksomhet på arbeidet som foregår i den skarpe enden, og ha fokus på hvordan arbeidet faktisk blir utført. Weick eksemplifiserer dette med at når en opplever nesten-ulykker, betyr ikke det at systemet er trygt ettersom det ikke ble en ulykke, men at systemet er utrygt ettersom det nesten ble en ulykke (Weick et al., 1999). En hindring for bred operasjonell bevissthet er perioder med produksjonspress og overbelastning (Rasmussen, 1997). En effektiv HRO evner å balansere ulike målsettinger, og innehar ekstraordinær sensitivitet i perioder med ekstra press og overbelastning for de ansatte. Operasjonell sensitivitet må sees i sammenheng med de fire andre kognitive prosessene for å oppnå denne årvåkenheten som kreves for å tolke situasjoner rett og håndtere de deretter (Weick & Sutcliffe, 2007; Weick et al., 1999).

4.Forpliktelse til resiliens (Commitment to resilience)

Resiliens handler om kapasiteten en organisasjon har til å håndtere overraskelser og farer etter at de har manifestert seg, og evne å gjenopprette driften (Weick & Sutcliffe, 2007). Dette innebærer å være opptatt av å både forebygge at uønskete hendelser oppstår, men samtidig forberede seg på å håndtere allerede oppståtte feil. Å håndtere overraskelser handler om å kontrollere de, ikke nødvendigvis eliminere de (Weick & Sutcliffe, 2007; Weick et al., 1999). En HRO venter ikke bare på at en feil skal oppstå for å håndtere den, men forbereder seg på de uunngåelige overraskelsene (Aven & Krohn, 2013). En HRO anerkjenner menneskelig feilbarlighet i samspill med upålitelig teknologi, og håndterer dette med å både fokusere på

forebygging og begrensning av feil. Forpliktelsen til resiliens vises blant annet igjennom at improvisering verdsettes (Weick et al., 1999). En effektiv HRO evner å bruke erfaringen den har i repertoaret sitt og samtidig evne å improvisere og tilpasse seg nye situasjoner. Dette innebærer å ha et ambivalent forhold til anvendbarheten av tidligere praksis, og å på en og samme tid både tro og tvile på deres tidligere erfaring. Dette handler om å kunne lære av tidligere hendelser, men samtidige tilpasse seg et dynamisk miljø (Weick et al., 1999).

5. Desentralisert struktur (Underspecification of structures)

I en HRO blir beslutninger tatt basert på kunnskap og kompetanse, istedenfor hierarkisk plassering i organisasjonen (Roberts et al., 1994 i Weick et al., 1999). I strenge hierarkiske beslutningsprosesser risikerer en at viktig og relevant informasjon ikke kommer frem til beslutningstaker, noe som kan resultere i «overordnete feil». En desentralisert struktur derimot, handler om at de som forstår situasjonen best skal være involvert i å håndtere den. Det innebærer også at det ikke er de samme personene som tar beslutninger i hver eneste krise, noe som også vil bidra til at en ikke bare gjentar løsninger som har vist seg å fungere før, men faktisk tilpasser håndteringen av hendelsen til den spesifikke situasjonen. De som arbeider i den spisse enden i organisasjonen har ofte en bedre situasjonsforståelse enn de som jobber høyere oppe i hierarkiet (Weick et al., 1999). Weick et al. (1999) argumenterer derfor for at organisasjonen bør ha en mer dynamisk beslutningsprosess. Det kjennetegnes ved å åpne det som vanligvis er en hierarkisk struktur opp for ekspertise til å delta i beslutningsprosessen når det trengs, og at personer fra ulike deler av systemet får muligheten til å utveksle viktig informasjon som kan styrke beslutningsgrunnlaget. En desentralisert struktur bidrar dermed til mer fleksibilitet, improvisasjon og tilpasningsdyktighet i organisasjonen (Weick et al., 1999).

3.4 Oppsummering av teori og forskningsspørsmål

Dette kapittelet har beskrevet grunnleggende prinsipper for risikostyring og ulike former for barrierer. Trefaktormodellen består av verdier, trusler og sårbarheter, og utgjør risikovurderingen for uønskete cyberhendelser. ROS-analyser er et verktøy for å sammenstille risikovurderingen og velge barrierer. Rosness et al., (2002) sin forståelse av barriere som enhver sikkerhetsfunksjon som har som hensikt å forhindre ulykker, danner utgangspunktet for hvordan en barriere er forstått i denne studien. Reason (1997) sitt begrep om myke barrierer er

dekkende for hva som utgjør en ikke-tekniske barriere. Hollnagel (2008) grupperer de myke barrierene i symbolske og immaterielle. På bakgrunn av nevnte teoretiske bidrag har jeg utviklet følgende forskningsspørsmål:

1. Hvordan bruker nettselskapene ikke-tekniske barrierer, og hvilken funksjon har barrierene i nettselskapenes cybersikkerhet?

Et nettselskap er et sosioteknisk-system som består av et samspill mellom mennesker, teknologi og organisasjon. Reason (1997) og Dekker (2006) viser til hvordan menneskelige feilhandlinger henger sammen med karakteristikker med det sosiotekniske-systemet mennesker opererer i, som f.eks. teknologiske og organisatoriske faktorer. Det kan tenkes at hvordan en forstår menneskelige feil påvirker hvordan man bruker barrierer i møte med mennesker. På bakgrunn av dette er følgende forskningsspørsmål lagt til grunn:

2. Hvilken betydning har nettselskapenes forståelse av menneskelige feilhandlinger for barrierestyring innen cybersikkerhet?

High Reliability Organizations (HRO) er organisasjoner som lykkes i å organisere barrierene sine på en måte som gjør at de unngår organisatoriske ulykker. Weick et al., (1999) operasjonaliserer sentrale karakteristikker til en HRO gjennom sine fem kognitive prosesser som utgjør en organisasjons kollektive bevissthet. Det kan tenkes at en nettselskapenes kollektive bevissthet vil påvirke påliteligheten til de ikke-tekniske barrierene. På bakgrunn av disse teoretiske bidragene er følgende forskningsspørsmål utarbeidet:

3. Hvilken betydning har nettselskapenes kollektive bevissthet på ikke-tekniske barrierers pålitelighet innen cybersikkerhet?

4.Metode

Følgende kapittel vil studiens forskningsstrategi- og metode presenteres og begrunnes. Kapittel 4 vil gjennomgå, og gjøre rede for de valgte metodiske tilnærmingene i denne studien, samt styrker og svakheter ved disse. Følgende vil studiens formål og forskningsdesign forklares,

deretter legges oppgavens datainnsamlingsprosess og datakilder frem. Datamaterialet samt oppgavens tolkninger og konklusjoner vil også gjennomgås i lys av validitet og relabilitet. Avslutningsvis vil oppgavens etiske betraktninger diskuteres.

4.1 Studiens formål og valg av forskningsdesign

Cybersikkerhet er et omfattende og tverrfaglig felt som kan studeres fra mange perspektiv (Albrechtsen & Hovden, 2011). Bakgrunnen for studien var et ønske om å undersøke cybersikkerhetsarbeidet i kraftsektoren fra et ikke-teknologisk perspektiv. Dette dannet videre utgangspunktet for studiens innledende formål, som var å undersøke hvilken betydning menneskelige og organisatoriske faktorer har på cybersikkerheten i nettselskap. Oppgavens problemstilling er derfor: «*Hvordan forstår nettselskaper betydningen av ikke-tekniske barrierer innen cybersikkerhet?*». Etter hvert som min forståelse av fenomenet jeg studerte har økt, har utforming av problemstilling og forskningsspørsmål blitt kontinuerlig endret. I denne studien ble det derfor valgt det som Neuman (2006) omtaler som et eksplorativt design. Dette er et fleksibelt design, som passer godt til tema det ikke har vært forsket mye på, eller som ikke er klart forstått (Neuman, 2006).

Selv om studien tok utgangspunkt i et eksplorativt design, ble det innledende arbeidet med studien påvirket av allerede etablert teori om blant annet risikostyring, beredskap og MTO-teori, med spesielt fokus på den menneskelige faktor. Utformingen av intervjuguiden ble påvirket av disse teoretiske perspektivene, ettersom jeg visste at det var enkelte temaer jeg ønsket å undersøke nærmere. Dette legger føringer for hvordan jeg som forsker forstår fenomenet som undersøkes (Thagaard, 2018). I den etterfølgende analysen av innsamlet data, har nye teoretiske perspektiv blitt lagt til grunn som følge av at respondentene har ledet meg inn på temaer. Studien befinner seg dermed i en mellomposisjon mellom et induktivt og et deduktivt design. Thagaard (2018) omtaler dette som en abduktiv tilnærming, noe som innebærer at analysen av data danner utgangspunkt for nye teoretiske perspektiv, men at en også tolker denne dataen i lys av eksisterende teori. Dette var hensiktsmessig ettersom det var ønskelig med et fleksibelt og åpent design, men samtidig en mulighet til å tidlig føre studien inn i et spor som jeg anså som mest relevant.

En vanlig kritikk mot deduktiv strategi er at en kan risikere at en i større grad får svar på hvordan den undersøkte oppfatter forskerens fortolkning av virkeligheten, istedenfor hvordan de undersøkte selv fortolker virkeligheten (Jacobsen, 2000). Denne studiens problemstilling forsøker å besvare hvordan nettselskaper forstår betydningen av ikke-tekniske barrierer innen

cybersikkerhet. Ettersom det er nettselskapenes egen forståelse som er i fokus, ville et lukket deduktivt design ikke vært hensiktsmessig, da det ville lagt for store begrensninger på hvilke data som var interessante. Samtidig kan en induktiv strategi kritiseres for at det er umulig å utforske et fenomen med helt åpent sinn, og forskeren må alltid gjøre en form for avgrensning, enten bevisst eller ubevisst (Jacobsen, 2000). Valg av tema, og undersøkelsesopplegg ble tidlig i prosessen påvirket av at jeg leste tidligere forskning relatert til cybersikkerhet og sikkerhet i kraftbransjen, samt min egen samfunnsfaglige bakgrunn. Med dette utgangspunktet var dermed den abduktive tilnærmingen mest hensiktsmessig.

4.2 Kvalitativ metode og intervju

For å oppnå kunnskap om, og forståelse for hvordan nettselskapene oppfatter betydningen av ikke-tekniske barrierer, ble det ansett som mest hensiktsmessig å bruke kvalitativ metode i denne studien. En kvalitativ tilnærming gir grunnlag for å fordype seg i det fenomenet en studerer (Aase og Fossåskaret, 2014). Den mest anvendte metoden innenfor kvalitativ forskning er intervju. Formålet med intervju er å få fyldig og omfattende kunnskap om hvordan mennesker opplever sin livssituasjon, eller hvilke synspunkter de har på temaet intervjuet handler om (Thagaard, 2018). Kvalitative intervju var derfor et naturlig valg ettersom jeg ønsket å oppnå en dybdeforståelse for nettselskapenes bruk av ikke-tekniske barrierer. Thagaard (2018) omtaler den kvalitative forskningsprosessen som fleksibel, ettersom arbeidet med de ulike delene av studien pågår parallelt. Dette viser seg blant annet i at problemstillingen har blitt endret flere ganger, og at dette har medført at valg av teori har blitt kontinuerlig revidert. Eksempelvis ble det i starten av studien arbeidet med en midlertid problemstilling som omhandlet menneskelige og organisatoriske faktorers betydning for cybersikkerheten i nettselskaper. Etter hvert ble problemstillingen tilspisset til å omhandle ikke-tekniske barrierer.

Hvis formålet med studien hadde vært å generalisere funnene for hele bransjen, kunne for eksempel en kvantitativ spørreundersøkelse vært benyttet. Dette ville gjort det mulig å kvantifisere innsamlet empiri, og å ha et større og mer representativt utvalg (Grønmo, 2004) Dette ville imidlertid ikke vært hensiktsmessig for å oppnå den dybdeforståelsen og nyansene, som vil kommet frem i en samtale med nettselskapene. Ettersom studien hadde et eksplorativt design, med stadig endring av problemstilling og forskningsspørsmål under utforskningen av fenomenet, ville det heller ikke fungert med en kvantitativ tilnærming.

Jacobsen (2000) beskriver ulike grader av strukturering av et intervju. Jeg har valgt å benytte meg av semistrukturerte intervju. Dette betyr at det ble utviklet en tematisk inndelt intervjuguide (**Vedlegg 1**) med ferdig formulerte spørsmål, men at jeg først og fremst behandlet intervjuene som en samtale som ikke fulgte noen fast struktur. Ettersom hensikten med studien var å forstå hvordan nettselskapene selv arbeider med cybersikkerhet, var det ikke ønskelig å være for låst til en intervjuguide, uten noen mulighet for å komme med oppfølgingsspørsmål. Intervjuguiden har vært i kontinuerlig endring ettersom respondentene ledet meg inn på temaer jeg ikke hadde tatt høyde for i intervjuguiden. Selv om jeg ønsket en fleksibel tilnærming til intervjuene, ønsket jeg også at samtalen skulle være rettet inn mot temaer jeg anså som relevant, og sikre at alle respondentene ble spurt om sentrale spørsmål. En semistrukturert tilnærming var derfor naturlig for å ivareta at samtalen ble både fleksibel, men også hadde en viss retning og struktur.

4.3 Datakilder

Mine primærdata kommer fra intervju med personer som arbeider i nettselskaper. I forstudien har jeg riktig nok benyttet meg av dokumenter (NVE-rapporter, NOUer, lover og forskrifter, samt tidligere forskning og lignende) for å øke min forståelse og kunnskap om tematikken, men disse er ikke benyttet i fremstillingen av resultatene.

Jeg har gjennomført til sammen fem kvalitative intervju med tre forskjellige nettselskap. Alle nettselskapene er av ulik størrelse med sin egen struktur og oppbygging. Dette gjør at nettselskapene også organiserer ansvaret for cybersikkerhet på forskjellige måter. Ifølge beredskapsforskriften er nettselskapene pålagt å utpeke en ansatt som skal ha funksjonen som IKT-sikkerhetskoordinator. Denne personen skal ha oversikt over IKT-sikkerhetsarbeidet i virksomheten, og inneha rollen som faglig kontaktpunkt til beredskapsmyndigheten vedrørende IKT-sikkerhet (Beredskapsforskriften, 2012, §2-2). De ulike nettselskapene benytter forskjellige navn på stillingstitlene som arbeider med cybersikkerhet, eller fungerer som IKT-sikkerhetskoordinator. **Tabell 1** presenteres respondentene som er intervjuet i denne studien. Respondentene vil omtales ved nettselskapets egen stillingstittel, etterfulgt av bokstaven (A, B eller C) etter hvilket nettselskap de tilhører. Respondenten som ivaretar funksjonen som IKT-sikkerhetskoordinator jf. Beredskapsforskriften er merket med «*».

Respondent	Stillingstittel
Nettselskap A	• IKT-sikkerhetskoordinator * • Beredskapskoordinator
Nettselskap B	• IT-sikkerhetssjef, IT og digitalisering • Chief information security officer (CISO)*
Nettselskap C	• IT-sjef *

Tabell 1 Oversikt over respondenter.

Respondentene er basert på et strategisk utvalg, som innebærer at de er valgt ut basert på forhåndsdefinerte kriterier og relevans (Thaagard, 2018). Det ble vektlagt respondenter som arbeider tett med cybersikkerhet i sitt daglige arbeid, og det var en forutsetning for å intervjue nettselskapene at vedkommende som innehar funksjonen som IKT-sikkerhetskoordinator ville la seg intervjue. I stor grad består respondentene av personell som jobber tett med cybersikkerhet, og som har nettselskapets hovedansvar innenfor cybersikkerhet. Unntaket er her nettselskap A sin beredskapskoordinator som ikke har noe direkte formelt ansvar for cybersikkerhet, men innehar lang erfaring fra virksomheten og god innsikt i nettselskapets sikkerhetsarbeid, inkludert opplæring innen cybersikkerhet.

To av intervjuene ble gjennomført ansikt til ansikt, et intervju ble gjennomført over telefon, mens to intervju ble gjennomført via Skype. Jeg fikk ikke muligheten til å se noen av respondentene mine som ble intervjuet over Skype på video, på grunn av henholdsvis tekniske problemer, og et ønske fra respondent om å ikke være på video. Respondentene fikk imidlertid observere video av meg under begge intervjuene. Dette gjorde at jeg mistet muligheten til å observere hvordan intervjuobjektet opptrådde underveis. Jacobsen (2000) sier det kan være vanskelig å oppnå et klima av fortrolighet i intervju som gjennomføres over telefon eller internett. Det viser seg ofte at det er lettere å oppnå en god og åpen samtale ved personlig intervju der respondentene snakker ansikt-til-ansikt. Det kan også argumenteres for at en går glipp av noen nyanser når en ikke kan observere ansiktsuttrykk eller kroppsspråket til respondenten under intervjuet (Jacobsen, 2000). Selv om jeg ikke hadde muligheten til å observere hvordan respondentene opptrådde under disse intervjuene, opplevde jeg ikke at intervjuene var annerledes, eller dårligere enn de to som ble gjennomført ansikt-til-ansikt. Samtlige intervju ble gjennomført mens intervjuobjektet var på jobb. De fleste intervjuene varte

rundt 1 time, der det korteste var på ca. 40 minutter, mens det lengste var på nærmere 100 minutter.

4.4 Validitet og reliabilitet

Begrepene validitet og relabilitet blir brukt om forskningens gyldighet og pålitelighet. Det finnes mange ulike måter å anvende begrepene på, og de har ulik mening i kvantitativ og kvalitativ forskning. Begrepene benyttes også på forskjellige måter i litteraturen om kvalitativ metode (Thagaard, 2018). Enkelte har tatt til ordet for å forkaste begrepene validitet og relabilitet i kvalitativ metode, ettersom de er basert på en kvantitativ logikk tilpasset kvantitativ metode (Thagaard, 1998 i Jacobsen, 2000). Jacobsen (2000) argumenterer for at det å kritisk drøfte gyldighet og pålitelighet, ikke betyr at en underkaster seg en kvantitativ logikk, men at det bare betyr at en forholder seg kritisk til kvaliteten på de data som er samlet inn. Dette betyr å drøfte om en har fått tak i de data vi ønsket å få tak i (intern gyldighet), og drøfte om dette kan overføres til andre sammenhenger (ekstern gyldighet). I tillegg må en drøfte om en kan stole på de data som er samlet inn (pålitelighet) (Jacobsen, 2000). I det følgende vil i hovedsak Jacobsen (2000) sin forståelse av begrepene ligges til grunn.

4.4.1 Validitet

Begrepet validitet knyttes til de resultatene forskningen presenterer, samt hvordan forskeren tolker datamaterialet. Validitet omhandler gyldigheten av forskerens tolkninger (Thagaard, 2018). Intern gyldighet handler om resultatene kan oppfattes som riktige, eller intersubjektive, som er det nærmeste en kommer sannhet (Jacobsen, 2000). Dette innebærer at forskeren må argumentere for gyldigheten av funnene sine (Thagaard, 2018). En vanlig måte å validere sine funn på er å konfrontere respondentene med sentrale funn og konklusjoner fra undersøkelsen, for å teste i hvilken grad respondentene kjenner seg igjen i de resultatene som presenteres. Denne type validering setter imidlertid store krav til respondentene, ved at de aktivt må gi tilbakemelding (Jacobsen, 2000). Alle respondentene signerte et samtykkeskjema (**vedlegg 2**), der de ble tilbudt å få lese transkripsjon, eller godkjenne den delen av teksten som inkluderte deres svar. Ingen respondenter ønsket å benytte seg av dette tilbudet. En kunne ha argumentert for at dette kunne ha styrket valideringen, dersom en eller flere av respondentene hadde gitt tilbakemelding på om de kjente seg igjen i resultatene, ettersom det kan forventes at respondentene kjenner det aktuelle fenomenet fra innsiden (Jacobsen, 2000). Denne formen for validering har imidlertid en klar begrensning ettersom en forskers oppgave også er å avdekke

forhold som respondentene ikke nødvendigvis er klar over. I denne studien blir respondentenes uttalelser tolket gjennom teori fra et fagfelt respondentene ikke har bakgrunn fra. Dermed kan et funn som en respondent ikke kjenner seg igjen i, likevel være gyldig (Jacobsen, 2000).

Spørsmålet om en har fått tak i de riktige kildene, handler også om validitet (Jacobsen, 2000). Mine intervjuobjekter består av personer som alle har lang erfaring innenfor bransjen, og som alle har god forståelse for sikkerhetsarbeidet som gjøres i nettselskapet. Jeg vil dermed argumentere for at intervjuobjektene er høyst relevante for å forstå sikkerhetsarbeidet i nettselskapene. Det kan imidlertid argumenteres for å at et større utvalg hadde gitt et mer utfyllende bilde og nyansert bilde av sikkerhetsarbeidet. Det er mange personer og aktører som er involvert i arbeidet med cybersikkerhet. Dette omfatter blant annet ledelsen i nettselskapet, systemeiere, underleverandører, personer i som arbeider i den skarpe enden i SCADA-systemene, og personer ansatt i administrasjonen. Dette er personer som kunne vært inkludert for å ytterligere belyse hvordan sikkerhetsarbeidet faktisk gjennomføres.

Selv om en har fått tak i de riktige kildene, er ikke det nødvendigvis sikkert at kildene har vilje til å gi fra seg riktig informasjon. En må alltid være åpen for at kilder ikke ønsker å fortelle sannheten, eller at de ønsker å framstille seg i et positivt lys (Jacobsen, 2000). Ettersom cybersikkerhet er et sensitivt tema, kan det være flere grunner til at respondentene ikke ønsker å fortelle åpent og detaljert om eksempelvis sårbarheter i IKT-systemer, eller feil som de ansatte gjør i arbeidshverdagen. Jeg opplevde at respondentene var komfortable med å dele informasjon, også om forhold som ikke var positive for virksomheten. Det styrker også validiteten at flere av uttalelsene gikk igjen hos flere respondenter fra forskjellige nettselskap (Jacobsen, 2000). Det var imidlertid en respondent som aktivt presiserte at han uttalte seg på generelt grunnlag ettersom han mente at detaljerte svar på spørsmålene ville kreve å oppgi kraftsensitiv informasjon[3]. Likevel opplevde jeg ikke denne respondentens svar som noe mindre detaljert enn de andre.

Ekstern validitet handler om overførbarhet fra en kontekst til en annen. Enkelte bruker begrepet i tilknytning til i hvilken grad en undersøkelse kan generaliseres (Jacobsen, 2000). Hensikten med denne studien har aldri vært å generalisere funnene til å gjelde hele populasjonen av ansatte i nettselskap. Forskeren kan likevel argumentere for hvilken overføringsverdi resultatene representerer (Thagaard, 2018). I denne studien er det gjennomført fem intervju med tre nettselskaper. I Norge er det over 120 nettselskap (NVE, 2019). Dette legger sine åpenbare

[3] Se **4.5 etiske betraktninger** for en nærmere gjennomgang av hensynet til kraftsensitiv informasjon.

begrensninger for hvilken grad en kan argumentere for at resultatene er overførbare til andre nettselskap med et så lite utvalg. Likevel observeres det at det er mange betraktninger som går igjen hos de fleste intervjuobjektene, og at de peker på mange av de samme truslene og erfaringene med de ulike barrierene. Hos alle nettselskap snakkes det om utfordringer knyttet til det å danne en forståelse av hva som utgjør kraftsensitiv informasjon, og flere viser til utfordringer med å tolke beredskapsforskriften. Dette kan peke i retning av noen generelle tendenser i bransjen, og at en kan tenke seg at andre nettselskap vil ha flere av de samme erfaringene.

Det viste seg å være svært utfordrende å finne respondenter som var villige til å delta som intervjuobjekt. Selv om respondentene har vært relevante for problemstillingen, og bidratt til verdifull innsikt om nettselskapenes cybersikkerhetsarbeid, kan det sees på som en svakhet at det bare er gjennomført 5 intervjuer. Jacobsen (2000) beskriver at det oppstår en form for «metning» i datainnsamlingen når en har gjennomført mange intervju. På det siste intervjuet var det tydelig at det var betydelig overlapp mellom de andre intervjuene og at avkastningen med flere intervju ble gradvis mindre. Jeg følte imidlertid ikke at dette metningsnivået ble oppnådd, ettersom det alltid kom frem ny informasjon i alle intervjuene. Hadde studien inkludert flere respondenter ville de empiriske funnene vært mer nyanserte og utfyllende noe som ville gitt en større overføringsverdi.

4.4.2 Reliabilitet

Begrepet relabilitet kan knyttes til begrepet pålitelighet, og handler om forskningen er utført på en tillitsvekkende måte (Jacobsen, 2000). Begrepet relabilitet blir i kvantitativ forskning knyttet til repliserbarhet, som vil si at resultatene kan reproduseres av en annen forsker (Thagarard, 2018). Thagaard (2018) argumenterer for at repliserbarhet ikke er relevant innenfor kvalitativ forskning. En bør likevel stille seg spørsmål om det er trekk ved selve undersøkelsen som har påvirket resultatene (Jacobsen, 2000).

Jacobsen (2000) beskriver ulike kontekseffekter som kan påvirke resultatene. Alle intervjuene ble gjennomført mens respondentene var på jobb, der de fleste foregikk på formiddagen. Alle intervjuene var også avtalt flere dager, eller uker i forveien. En kan derfor si at intervjuobjektene hadde mulighet til å være forberedt på intervjuet.

En trussel mot troverdigheten til datamaterialet, er at forskeren har vært slurvete i registreringen av data (Jacobsen, 2000). Det ble spilt inn lydopptak av alle intervjuene, noe som gjorde transkriberingen vesentlig mer presis enn om den skulle vært basert på notater. En kan likevel

stille spørsmål om nøyaktigheten av analysen av data. En sentral del av analysen er å kategorisere og forstå dataen for å etablere sammenhenger (Jacobsen, 2000). I dette arbeidet vil det alltid være et element av skjønn som avgjør hvordan data kategoriseres. Det kan sees på som en svakhet at jeg ikke har bakgrunn fra verken IKT eller elkraft. Dette opplyste jeg respondentene om for å sørge for at deres svar ble sagt på en lett forståelig måte. Det kan likevel ikke utelukkes at det har forekommet misforståelser, eller at jeg har tolket enkelte deler av dataen upresist.

I en diskusjon om relabilitet drøftes ofte spørsmålet om i hvilken grad ledende spørsmål har påvirket respondentene (Kvale & Brinkmann, 2015). Kvale & Brinkmann (2015) hevder at det er veldokumentert at små justeringer på spørsmålsformuleringen vil påvirke hvordan respondentene svarer. Thagaard (2018) mener at bruk av ledende spørsmål bidrar til at til å begrense intervjupersonens svaralternativ, og skaper en forventning til hvordan intervjuobjektene skal svare på spørsmålet. Bruk av ledende spørsmål bør derfor unngås, og en bør heller formulere åpne spørsmål for å få mer autentiske svar (Thagaard, 2018). Under utformingen av intervjuguiden forsøkte jeg å begrense bruk av ledende spørsmål, men ettersom jeg benyttet et samtalebasert intervjuformat ble det både bevisst og ubevisst benyttet ledende spørsmål. Kvale & Brinkmann (2015) hevder imidlertid at bruk av ledende spørsmål også kan bidra til å styrke relabiliteten, og kan benyttes for å verifisere intervjuerens fortolkning. Under intervjuene opplevde jeg flere ganger at det var nødvendig å stille ledende og direkte spørsmål for å forsikre meg om at jeg hadde forstått respondentene rett. Det ble også benyttet ledende spørsmål for å forsikre at respondentene forstod mine spørsmål rett. Dette gjaldt blant annet i spørsmål knyttet til risikostyring og beredskap, der det flere ganger viste seg at jeg og intervjuobjektene hadde en ulik tilnærming til begrepene. Jeg vil dermed argumentere for at bruk av ledende spørsmål har bidratt til å styrke relabiliteten, men det kan ikke utelukkes at dette ubevisst har påvirket respondentenes forventinger til svaralternativer, slik Thagaard (2018) beskriver.

4.5 Etiske betraktninger

Samtlige respondenter har signert et samtykkeskjema der de ble informert om at intervjuet ble tatt opp på bånd. Det ble også informert om at alle respondenter og virksomheter som deltok i studien skulle anonymiseres. Dette var for å sikre at ingenting som ble sagt under intervjuene skulle slå negativt ut på virksomheten. Det er et grunnleggende forskningsetisk prinsipp at

deltagelse i forskning, ikke skal ha noen negative konsekvenser (NESH, 2016 i Thagaard, 2018). Som forsker har jeg derfor et ansvar for at sensitiv informasjon ikke skal publiseres, og jeg ønsket derfor ikke å stille spørsmål som kunne gi sensitive opplysninger. Kraftberedskapsforskriften (2012) § 6-2 omtaler kraftsensitiv informasjon som:

> *«Med kraftsensitiv informasjon menes spesifikk og inngående opplysninger om kraftforsyningen som kan brukes til å skade anlegg, system eller annet eller påvirke funksjoner som har betydning for kraftforsyningen …» (Kraftberedskapsforskriften, 2012, § 6-2)*

Et av de sentrale funnene i studien er at det var ulik forståelse for hva som utgjør kraftsensitiv informasjon innad i nettselskapene. Dette viste seg å ha både etiske og metodiske implikasjoner for studien. En av respondentene hadde en tydelig mer defensiv innstilling under intervjuet, og utpekte seg som mer varsom med hvor detaljert han ville svare på spørsmålene av hensyn til kraftsensitiv informasjon. Han besvarte imidlertid alle spørsmålene, og han fikk stort sett de samme spørsmålene som de andre respondentene. Han presiserte dog aktivt at han besvarte de på generelt grunnlag, men svarene fremstod likevel like detaljerte som de andre. Ingen av de andre respondentene hadde noen innsigelser på valg av spørsmål, og fremstod som mer komfortable under intervjuet.

Alle respondentene ble tilbudt å lese igjennom transkripsjon av intervjuet, eller få lese deres svar som skal benyttes i studien. Dette var gunstig for å sørge for at respondentene fikk tillit til meg som forsker, og at det ble mulighet for å endre, eller trekke tilbake ting som ble sagt under intervjuet. Alle respondentene var også orientert om at studien kunne publiseres på internett, og at de at de opplysningene som kom frem under intervjuet kunne benyttes i studien.

Et annet grunnleggende forskningsetisk prinsipp, er prinsippet om informert samtykke (Thagaard, 2018). Den fleksibiliteten som preger kvalitative studier, innebærer at det er vanskelig for deltakere å vite hva de egentlig samtykker til. Verken forsker eller deltaker kan forutsi utviklingen av forskningsprosjektet (Thagaard, 2018). Selv om alle deltakerne arbeider med sikkerhet, har de selv en annen faglig bakgrunn enn meg. Deltakerne kan dermed oppleve at resultatene fra undersøkelsen vil settes inn i en faglig sammenheng som kan oppleves som fremmed i forhold til den forståelse de har av sin egen situasjon (Thagaard, 2018). Det har derfor vært viktig for meg å informere deltakerne om hva som var hensikten med studien. Det er likevel et spørsmål om i hvilken grad en kan oppnå informert samtykke innen kvalitativ

forskning. Selv om deltakerne har gitt sitt samtykke, betyr ikke det nødvendigvis at deltakere i etterkant av prosjektet er komfortable med sin deltakelse (Thagaard, 2018).

5.Empiri

I dette kapittelet presenteres hovedfunnene fra intervjuene med respondenter fra ulike nettselskap. **5.1** presenter respondentenes erfaringer med ulike cyberhendelser og oppfatninger om trusselbildet innenfor cybersikkerhet. **5.2** presenteres nettselskapenes erfaring med risikostyring av cybersikkerhet med fokus på ROS-analyser og barrierer. **5.3** redegjør for nettselskapenes betraktninger om den menneskelige faktor innenfor cybersikkerhet, herunder hvilke feil som begås og hvorfor feilene begås. **5.4** viser til ulike organisatoriske cybersikkerhetstiltak.

5.1 Cyber-trusselbildet

Kraftbransjen i Norge har ikke blitt utsatt for noen vellykkete angrep av typen vi har sett i Ukraina, og cyberangrep mot norske aktører har heller ikke medført strømavbrudd. Respondentene er likevel åpen for at lignende angrep kan skje i deres virksomhet, og de er derfor opptatt av å etablere barrierer mot ulike former for cyberangrep. De uønskede IKT-hendelsene som har rammet virksomhetene har derfor ikke hatt konsekvenser for energiforsyningen. De uønskede hendelsene som forekommer utgjør likevel en risiko for at kraftsensitiv informasjon kan lekkes, og dermed potensielt ramme energiforsyningen. Av uønskede hendelser som har oppstått er det primært snakk om phishing-angrep der sluttbruker har trykket på skadelige lenker. To virksomheter har vært utsatt for løspengevirus, men dette fikk ikke større konsekvenser enn noen tapte arbeidstimer for å få filene tilbake fra back-up.

Omfanget av phishing-eposter er imidlertid stort, og alle virksomhetene opplever at ansatte trykker på ugunstige lenker. I nettselskap B observeres det sjeldent skadevare direkte på e-posten ettersom flere tekniske barrierer filtrerer ut de skadelige vedleggene. De fleste av angrepene er masseproduserte angrep som ikke nødvendigvis er målrettet. Alle virksomheter har likevel erfaringer med målrettete, skreddersydde eposter. Alle nettselskap har vært utsatt for forsøk på CEO-svindel, men dette har vært mislykket fra angripernes side. Selv om ikke konsekvensen av phishing-angrepene har vært store, er epost en potensiell sårbarhet som kan

utnyttes for større angrep, som f.eks. angrepet i Ukraina demonstrerte, noe også respondentene anerkjenner.

Alle respondentene forteller at de forholder seg til myndighetenes årlige trusselvurderinger. Her nevnes PST, Etterretningstjenesten, Kripos, NSM og NVE sine rapporter om risiko og trusselvurderinger. Respondentene ser på statlige etteretningsoperasjoner som en trussel, og spesielt Russland og Kina nevnes hyppig av respondentene. Her er både og informasjon om kritisk infrastruktur og bedriftshemmeligheter informasjon som må beskyttes. Også enslige amatørhackere nevnes som en potensiell trussel, men det er først og fremst profesjonelle hackere nettselskapene er bekymret for. Samarbeidspartnere som KraftCERT og FSK (Forum for informasjonssikkerhet i kraftforsyningen) er viktige for nettselskapene for å få kontinuerlig oppdatering om trusselbildet.

5.2 Risikostyring

De fleste av respondentene har risikostyring av informasjonssikkerhet som et av sine hovedansvarsområder. Respondentene ble spurt om deres forståelse av begrepet risikostyring. IKT-sikkerhetskoordinator A hevder at risikostyring handler om å ha rutiner for å analysere risiko, og vite hvilke trusler en er utsatt for slik at en kan sørge for at tiltak innføres og identifisere hvilken risiko som er akseptabel. IT-sikkerhetssjef B sier risikostyring kan sees på som et samlebegrep på hva som gjøres for å kontinuerlig forbedre informasjonssikkerheten. IT-sjef C knytter begrepet risikostyring til det rammeverket som nettselskapet har implementert for å sikre, overvåke og vedlikeholde et helhetlig bilde av risikoen nettselskapet eksponeres for.

Respondentene ble spurt om hvilke aktiviteter som inngår i risikostyringen. Her nevnes risikovurdering som handler om identifisering av uønskete hendelser og å etablere en oversikt over risikobildet. Risikohåndtering forklares som tiltaksoppfølging og kartlegging av etterlevelsen av de ulike risikoreduserende tiltakene. Som en del av risikohåndteringen nevnes også det å ha sikkerhetsovervåkning og hendelseshåndtering. Arbeid med kompetanse, brukerbevissthet og utvikling av en sikkerhetskultur regnes også som en del av virksomhetenes risikostyring ifølge IT-sikkerhetssjef B.

I nettselskap B foregår det et større prosjekt for å klassifisere kraftsensitiv informasjon, og i nettselskap A er det også planlagt en omfattende gjennomgang av hvordan en skal klassifisere kraftsensitiv informasjon. Hensikten med prosjektet i nettselskap B er ikke bare å avgjøre hva

det er som er å anse som kraftsensitiv informasjon, men også å vurdere hvilken verdi informasjonen har, hva som er å anse som beskyttelsesverdig, og hvilke grader av beskyttelses denne informasjon skal ha. CISO B hevder det er ganske ulik oppfattelse innad i nettselskapet om hva som er beskyttelsesverdig og hva som ikke er, og det er derfor en prioritert oppgave i handlingsplanene å arbeide med en bedre klassifisering av informasjon. Ulike oppfatninger om hva det er som er å anse som sensitiv informasjon er også et tema i de andre nettselskapene. IKT-sikkerhetskoordinator A sier at manglende forståelse blant ansatte for hva som utgjør kraftsensitiv informasjon kan føre til at en laster opp denne informasjonen i eksterne IT-systemer, som uvedkommende kan få tilgang til.

5.2.1 ROS-analyser

Respondentene sier at ulike former for ROS-analyser er sentralt i arbeidet med risikostyring av cybersikkerhet. Det brukes mye tid på risikovurderinger i nettselskapene, og det er enighet om at ROS-analyser er et nyttig verktøy i dette arbeidet. Risikoanalysene beskrives som nyttige for å skape en felles bevissthet i organisasjonen om trusler og sårbarheter. Det er også et krav i nettselskapene om å utføre risikoanalyser før store endringer kan finne sted. Alle nye IT-tjenester eller endring av systemer skal dermed risikovurderes. IKT-sikkerhetskoordinator A forteller at risikoanalysene har sin styrke når det kommer til å kartlegge og identifisere hendelser som kan skje. Han påpeker videre viktigheten av at risikoanalysene følges opp med konkrete tiltak med tidsfrister for når tiltakene skal være fulgt opp, og tildele ansvar for hvem som skal iverksette tiltakene. Han føler at det som blir avdekket i risikoanalysene i all hovedsak blir fulgt opp. I nettselskap A deltar en rekke ulike fagfolk som har ekspertise på systemene som skal risikovurderes, i tillegg til egne fasilitatorer som har ekspertise på risikoanalysene, samt øvrig IT-personell.

I virksomhet B hevder deres CISO at det er svakheter med oppfølgingen av tiltakene. Det gjøres mange risikovurderinger, men at resultatene av disse ikke alltid rapporteres til ulike ledere, noe som gjør at de som er ansvarlig ikke kjenner til risikoen. Han sier det er et problem at mange risikovurderinger «*… ender opp i en skuff*». IT-sjef C sier at selve prosessen med å lage risikoanalyser i seg selv alltid har en stor positiv verdi, ettersom det innebærer at sentrale fagpersoner går sammen og kommuniserer med hverandre om trusler og tiltak.

Respondentene trekker også frem en rekke utfordringer knyttet til bruken av ROS-analyser. IKT-sikkerhetskoordinator A sier det er en utfordring å kommunisere at ting som ikke har hendt før likevel kan skje. Han trekker frem at det aldri har skjedd strømavbrudd i Norge som følge

av cyberangrep, men sier at dette fortsatt kan inntreffe. Dette er også vanskelig å kommunisere via en ROS-analyse. Han knytter dette til utfordringer ved fastsettelse av risikonivå. Hendelser som ikke har hendt før vil ofte bli vurdert som noe som har svært liten sannsynlighet for å skje, men konsekvensene kan likevel være katastrofale. Slike hendelser kan være vanskelig å fastsette et passende risikonivå for, og det uttales at de «*bare må bli enig om noe*». CISO B trekker også frem problemer med å fastsette risiko og spesielt sannsynlighetsberegning er veldig vanskelig. Han sier at det er tilnærmet håpløst å fastsette et sannsynlighetsnivå på hendelser som en ikke har erfaring med. IT-sjef C sier at når en skal fastsette sannsynlighet innen cybersikkerhet, mangler det ofte relevant statistikk for å underbygge sannsynlighetsestimatet.

IKT-sikkerhetskoordinator A fremhever viktigheten av å tilpasse risikoanalysene til IT-system. Han illustrerer dette med et eksempel som viser forskjellen i volumet av antall hendelser som skjer innen IKT sammenlignet med resten av bransjen. Han sier at i kraftbransjen er de mest risikofylte hendelsene de som skjer hvert år, mens de minst risikofylte er de som skjer hvert 1000. år. Innen IKT-sikkerhet må dette tilpasses, og han sier at de mest risikofylte hendelsene er de som skjer hver dag, mens de som er minst risikofylte er de som skjer ca. hvert 10. år.

Nettselskapene benytter risikoakseptkriterier, og hevder det er viktig for risikostyringen, men IT-sikkerhetssjef B sier at kontinuerlig forbedring også er et viktig stikkord knyttet til risikostyringsprosessen. CISO B hevder at deres virksomhet har mangelfull bruk av risikoakseptkriterier. Han sier det er et problem at det brukes ulike risikoakseptkriterier på ulike prosjekt og deler av organisasjonen, og at selv om det har vært en positiv utvikling, har de likevel en lang vei å gå. Alle tre nettselskapene henviser til risikomatrisen som verktøy for risikoaksept.

CISO B hevder at han prøver å kommunisere i organisasjonen at risikostyring er deres viktigste verktøy. Han mener imidlertid at kvaliteten på risikostyringen kunne vært bedre, og opplever blant annet at det er utfordrende at ikke alle har samme forståelse av begrepene eller snakker samme språk. Han illustrerer dette med eksempler på at noen blander sammen en sårbarhet med en konsekvens, og en risikobetraktning med en trussel. IT-sjef C mener at også deres nettselskap har forbedringspotensialet for risikostyringsprosessen. Han hevder at det ikke er strukturert nok, og det er en felles enighet i ledelsen om at det ikke eksisterer gode nok rutiner og rammeverk for god risikokommunikasjon av cybersikkerhet til styret, noe som kan medføre at det kan bli vanskelig å danne en felles forståelse av risiko. Det jobbes derfor med å etablere en praksis for risikokommunikasjon av cybersikkerhet til ledelsen.

5.2.2 Barrierer

Respondentene ser på det å etablere barrierer som en viktig del av risikostyringen. Beredskapskoordinator A sier at risikostyring er nært tilknyttet det å etablere barrierer for å styre risiko. Alle respondentene benytter barrierebegrepet aktivt, og begrenser det ikke bare til fysiske og tekniske tiltak, men også til organisatoriske og menneskelige tiltak. Selv om respondentene sier at de tekniske barrierene er mange og gode, er alle opptatt av at de tekniske barrierene aldri vil kunne gi 100% sikkerhet. IT-sikkerhetssjef B sier at aktører med ubegrenset tid og ressurser har muligheter til å forsere barrierer, derfor trengs det andre mekanismer som ivaretar evnen å identifisere og oppdage unormal aktivitet. Ettersom trusselaktørene kan tilpasse seg barrierene, er det vanskelig å holde de tekniske barrierene oppdaterte. Barrierer som f.eks. stopper uønsket e-post den ene dagen stopper det ikke nødvendigvis i morgen sier IT-sikkerhetssjef B.

IT-sikkerhetssjef B sier at barrierene deres er organisert etter prinsippet om forsvar-i-dybden. Med dette mener at han at barrierene er organisert i flere lag, og at dersom en eller flere av barrierene blir passert, skal andre barrierer kunne forhindre den uønskete hendelsen. Han sier at et viktig ledd i dette arbeidet er å anerkjenne at ingen barrierer er 100% sikre. Han hevder at summen av flere tekniske og organisatoriske barrierer sammen skal kunne gi en god beskyttelse, men at en alltid må forsøke å forbedre barrierene. *«Fravær av uønskete hendelser og FLAKS er ikke noen god styringsparameter …»*. Et ledd i dette arbeidet er å følge med på hendelser i samfunnet ellers og erkjenne at hendelser andre opplever også kan ramme en selv. Det jobbes derfor kontinuerlig med beredskapsarbeid og beredskapsplaner i tilfelle noen av de sannsynlighetsreduserende barrierene skulle svikte. I dette arbeidet innebærer det å arbeide med rutiner for hvordan en skal varsle om og håndtere uønskete IKT-hendelser. Det arrangeres beredskapsøvelser ved jevne mellomrom, der de øver på IKT-hendelser. CISO B sier de arbeider med å etablere rutiner for hvem som skal være en del av hendelseshåndteringsteamet i beredskapssituasjoner og at det er planlagt øvelser relatert til dette.

Alle respondentene snakker om at mennesker kan fungere som en barriere, og mye av sikkerhetsarbeidet går ut på å danne barrierer mot menneskelige feilhandlinger. En del av dette arbeidet er å lære opp de ansatte og gjøre de mer bevisste om risiko. IT-sikkerhetssjef B sier *«Jeg gjør det veldig tydelig ovenfor brukere at dere er den siste sikkerhetsbarrieren, og prøver å gjøre de litt stolte av det»*. Selv om det finnes tekniske barrierer som begrenser handlingsrommet til de ansatte, (e-post filter, frata administratorrettigheter, ikke godkjenne diverse typer vedlegg og programmer) har de ansatte likevel et betydelig ansvar for å ha korrekt

sikkerhetsadferd i arbeidshverdagen. CISO B sier de er avhengig av at brukerne tenker seg godt om i hverdagen ettersom avdelingen for informasjonssikkerhet av består av to personer, og de ikke kan være overalt. IT-sjef C sier at i tillegg til tekniske sikkerhetsløsninger er kultur og bevissthet svært viktig for at sikkerheten ivaretas.

5.3 Menneskelig faktor

5.3.1 Menneskelig feilhandlinger

Alle respondentene er opptatt av at mennesker er det siste sikkerhetsleddet i organisasjonen og de bruker mye tid på å bevisstgjøre de ansatte om at cybersikkerhet er et felles ansvar. Å redusere menneskelige feilhandlinger blir dermed en viktig del av cybersikkerhetsarbeidet for nettselskapene. Alle respondentene sier at de mest vanlige feilene de ansatte gjør, er å trykke på phishing-lenker. IT-sikkerhetssjef B sier at e-post var metoden som ble brukt da de ble rammet av løspengevirus for noen år siden, da en ansatt trykket på en skadelig lenke. Han forteller at de kan se på loggene at det fortsatt forekommer klikk på lenker som kan utgjøre en risiko, men at de ikke har hatt uønskete hendelser som følge av dette de siste to årene. Han sier videre at de neppe har full oversikt over alle uønskede klikk på phishing-lenker, men at han opplever at brukerne generelt er årvåkne. Det hender imidlertid at brukere først trykker på lenker, men deretter våkner når de blir bedt om å oppgi brukernavn og passord. IT-sjef C sier at en ansatt trykket på en phishing-lenke og endte opp med å oppgi både brukernavn og passord, men at han meldte inn dette til IT-avdelingen år han skjønte at han hadde begått en feil.

En annen vanlig feil som hyppig nevnes av respondentene er at de ansatte laster opp kraftsensitiv informasjon på feil plasser. Mange skytjenester er ikke regnet som sikker nok til at kraftsensitiv informasjon kan lagres der, men dette forekommer likevel. IKT-sikkerhetskoordinator A hevder at det generelt deles for mye kraftsensitiv informasjon over internett uten at de ansatte tenker godt nok over om de som deler informasjonen med, faktisk trenger all denne informasjonen. Nettselskap B og C regner også med at ukryptert kraftsensitiv informasjon sendes over e-post selv om dette ikke er tillat.

IKT-sikkerhetskoordinator i nettselskap A og IT-sikkerhetssjef B forteller begge at de tidligere har hatt problemer med svake holdninger til passord, og slurv med dette. De illustrerer dette med eksempler der ansatte har benyttet seg av svake passord, eller gjenbrukt for mange gamle passord. Det blir også trukket frem eksempler på at ansatte skriver ned passord på lapper som

ligger synlig på kontoret, og at ansatte deler brukere med hverandre. IT-sikkerhetssjef B forteller at det er et problem at ansatte stadig finner nye måter å benytte seg av programvare og tjenester som ikke er godkjent av ledelsen («skyggetjenester»). Å frata vanlige sluttbrukere administratorrettigheter er en teknisk barriere som hindrer omfanget av bruk av skyggetjenester, men brukere som ønsker en enklere arbeidshverdag er kreative og finner måter å omgå barrierene på og benytte seg av tjenester som ikke er tillat.

CISO B sier at den kanskje største, og mest alvorlige feilen er at i utarbeidelsen av ulike prosjekter der det lages nye systemer, så blir det ikke godt nok gjennomtenkt hvilken type informasjon dette systemet skal behandle. Han sier at de som utarbeider systemene er veldig opptatt av hvilken funksjonalitet et system skal ha, men at en ikke har et bevisst nok forhold til hvilken informasjon som skal flyte i dette systemet og hvilken beskyttelse den trenger. Som en konsekvens av dette blir ikke sikkerhet tatt med tidlig nok i vurderingen, ettersom en ikke er har god nok bevissthet om hvilken informasjon som er beskyttelsesverdig.

5.3.2 Hvorfor begår mennesker feilhandlinger?

Respondentene ble spurt om hvorfor de tror ansatte gjør feil. IKT-sikkerhetskoordinator A sier de har et stort fokus på opplæring innen IKT-sikkerhet, men at mangler i opplæringen kanskje likevel er den viktigste årsaken til at folk begår feil. Det er også stor forskjell på hvor stor opplæring enkelte trenger: noen trenger knapt opplæring, mens andre trenger mye opplæring. Det er vanskelig å lage et generelt opplæringsprogram som passer for alle, og det kan også være vanskeligheter med å identifisere hvem det er som trenger ekstra hjelp**.** Han sier det også er krevende å bevisstgjøre alle ansatte mot alle trusler og hvilken informasjon som er beskyttelsesverdig. CISO B hevder også at opplæringen kan forbedres og sier at både montører, og kontoransatte har etterlyst mer opplæring, ettersom de selv hevder de ikke har en god nok forståelse for cybersikkerhet.

Beredskapskoordinator A, samt IT-sikkerhetssjef B hevder at i en hektisk hverdag kan det tenkes at det er fort forekommer uønskete klikk, spesielt med tanke på hvor mange ansatte det er, og hvor mange e-poster de må forholde seg til. Tidspress og ønske om en enklere hverdag er også en av grunnene til at ansatte velger å bruke skyggetjenester som ikke er godkjent, ifølge IT-sikkerhetssjef B. Svake holdninger til passord og protester mot krav til komplekse passord kan også forklares med et ønske om en enklere, og mer effektiv arbeidshverdag. IKT-sikkerhetskoordinator A hevder at det er en utfordring at eksterne IT-systemer som Office 365 er mer brukervennlige enn nettselskapets egne systemer, noe som medfører at brukere velger å

lagre kraftsensitiv informasjon på eksterne system, istedenfor interne system som er regelen. Respondentene forteller at det er en vanskelig avveining mellom frihet og brukervennlighet på den ene siden, og sikkerhet på den andre. Det er ikke ønskelig å overvåke alt de ansatte foretar seg, i tillegg er det nødvendig å legge til rette for at tjenestene er brukervennlige. IT-sjef C sier at dersom f.eks. det oppfattes som «*et herk*» å kryptere sensitiv informasjon før de sendes over e-post, vil kanskje ikke de ansatte ta seg tid til å kryptere informasjonen. IKT-sikkerhetskoordinator A sa at de tidligere brukte et e-post filter som skulle ta vekk spam og svindel, men at dette filteret var så aggressivt at det også filtrerte vekk legitime e-poster som var ønsket. På grunn av hensyn til brukervennlighet ble derfor dette filteret tatt vekk, og de ansatte blir dermed eksponert for flere phishing-forsøk igjen.

IT-sikkerhetssjef B forteller at selv om de kontinuerlig arbeider med å få de ansatte til å gjøre mindre feil, er det urealistisk å noen gang oppnå 100% menneskelig pålitelighet. IKT-sikkerhetskoordinator A sier at en del av phishing-forsøkene er så sofistikerte at selv folk på IT-avdelingen blir lurt til å trykke på lenkene, noe som illustrerer utfordringen med å få ansatte til å unngå å gjøre feil. Kompleksiteten av cybertruslene, og selve volumet av hendelser blir brukt av respondentene som årsaker til hvorfor det forekommer menneskelige feilhandlinger.

IKT-sikkerhetskoordinator A trekker imidlertid også frem ulik risikoaksept og at personlighetstyper blant de ansatte også kan være en faktor for hvorfor det begås feil. Han utdyper dette med at enkelte generelt har en svak holdning til sikkerhet og informasjonssikkerhet, og sammenligner dette med folk som kjører i 130 kilometer i timen på motorveien. Flere respondenter trekker frem ulike karakteristikker med de ansatte som gjør at de er mindre interessert og har mindre kompetanse på cybersikkerhet. Manglende utdannelse innen IKT, og erfaring med IKT som følge av høy alder blir pekt på som årsaker til at enkelte kan være mer disponert for å gjøre feil og generelt mindre interesse for å oppsøke, og tilegne seg informasjon om cybersikkerhet.

Respondentene trekker frem manglende bevissthet og risikoforståelse som mulige årsaker til at ansatte gjør feil. Flere av respondentene hevder at manglende forståelse for IKT blant de ansatte gjør at de ikke forstår de tekniske implikasjonene av valgene de foretar seg på datamaskinen. IT-sjef C tror at manglende forståelse av risiko er en av de viktigste årsakene til at folk kan gjøre feil. Han illustrerer dette med eksempler på at han ikke tror alle har teknisk innsikt i hvilken risiko det er å lagre sensitiv informasjon i skytjenester, eller å sende ukryptert sensitiv informasjon på e-post. IT-sikkerhetssjef B sier dog at han ikke tror man kan skylde for mye på manglende risikoforståelse ettersom han mener de ansatte allerede er godt opplærte og årvåkne

om risiko. Han mener at de ansatte heller gjør feil fordi det er en hektisk hverdag og at de derfor glemmer å tenke seg om.

I alle nettselskapene nevner respondentene at det er en utfordring å skape en felles forståelse over hva som utgjør kraftsensitiv informasjon, og at dette er med på å gjøre det mer sannsynlig for at mennesker gjør feil. CISO B tenker at det er på grunn av manglende forståelse av hva som er å anse som sensitiv informasjon at sikkerhet og beskyttelse av informasjon ikke blir tidlig nok ivaretatt under utarbeidelsen av nye system. Han sier dette er et symptom på et det tidligere ikke har vært gjort en grundig nok klassifisering av informasjon i nettselskapet, og at det derfor nå foregår et stort prosjekt der en klassifiserer informasjon som er beskyttelsesverdig. Manglende forståelse av informasjonsverdi blir også trukket frem av andre respondenter som hevder at dette kan bidra til at en velger å laste opp kraftsensitiv informasjon på eksterne sky-tjenester som ikke er godkjent, eller sender ukryptert på e-post.

5.4 Organisatoriske cybersikkerhetstiltak

5.4.1 Opplæring innen cybersikkerhet

Alle ansatte må igjennom en obligatorisk cybersikkerhetsopplæring, men det varierer hvor omfattende denne er i de ulike nettselskapene. I alle nettselskapene kurses jevnlig de ansatte i nettselskapene gjennom sikkerhetsmåneder, interne og eksterne foredrag, e-læring og lignende. Om E-læring blir det spesielt framhevet at det benyttes korte obligatoriske videosnutter som er bevisst laget korte og enkle, slik at det ikke blir så mye å gå igjennom hver gang. Nettselskapene har oversikt over hvem som har klikket seg igjennom videosnuttene og sender purringer dersom enkelte ikke har klikket igjennom innholdet. E-læringen fokuserer blant annet på hvordan kjenne igjen phishing-eposter. CISO B er imidlertid skeptisk til effekten av e-læring, selv om han ønsker at de skal fortsette å benytte seg av det. Han har inntrykk av at enkelte ansatte bare klikker seg raskt igjennom innholdet og så glemmer alt de har lært, og at det neppe er et format som klarer å fange opp interessen til alle. Han ser istedenfor en større verdi i å gå ut å oppsøke mennesker på ulike avdelinger, og snakke med dem om hva det er de trenger hjelp til. Slik kan han både gi og få innspill til hva som fungerer, og få et bedre innblikk i hva den enkelte sliter med. Han mener at dette henger sammen med at mennesker er forskjellige, med ulike personlighetstyper, og derfor vil ikke en standardisert opplæring fange opp alle. *«… Du vet egentlig ikke hva slags utfordringer den enkelte person har før du har snakket med de»*

Alle nettselskapene har et eget forum om informasjonssikkerhet på intranett, men i nettselskap A er det ikke obligatorisk å abonnere på denne informasjonen om informasjonssikkerhet. Beredskapskoordinator i selskap A mener informasjonen som kommer ut på intranett er både god og nyttig, men han tror at de som hadde hatt mest bruk for informasjonen er de som ikke abonnerer på forumet. Dette bekrefter også IKT-sikkerhetskoordinatoren som hevder at det gjerne er de som allerede er interessert i cybersikkerhet som abonnerer, og at det er de som ikke er interessert som utgjør størst risiko. Han sier det også er en utfordring i å vite hvor mye informasjon man skal legge ut på intranettet om cybersikkerhet før folk blir «mette», ettersom det er mye annen informasjon som ikke er relatert til cybersikkerhet de også må forholde seg til. IT-sikkerhetssjef B sier at en må være varsom mot å rope «ulv, ulv», for å opprettholde interessen fra de ansatte for det som publiseres på intranett. CISO B hevder at ettersom selskapet har flere mål enn bare sikkerhet, har det resultert i at selve informasjonsmengden på intranett er altfor stor. Dette fører til at informasjonen om cybersikkerhet kun blir lest og forstått av de som allerede er interessert i temaet, mens andre ikke leser den.

IT-sikkerhetssjef B sier at arbeidet med å utvikle virksomhetens sikkerhetskultur er meget viktig, og er et kontinuerlig arbeid som utføres blant annet gjennom opplæring og undervisning. Opplæringen foregår blant annet via internett, men det arrangeres også møter med gruppeundervisning. Han forsøker å informere ansatte om eksterne hendelser for å bruke dette som eksempel på hva som kan ramme egen virksomhet. Selv om en ikke alltid har et fullstendig bilde over hva som er årsakene til eksterne hendelser, forsøker han å fremheve hva vanlige brukere kan gjøre for å redusere risikoen for at slike hendelser oppstår. På den måten får de større oppmerksomhet rundt cybersikkerhet, og brukerne forstår bedre hvorfor de er så opptatt av det. Etter cyberangrepet mot Hydro ble det umiddelbart mer undervisning om risiko knyttet til lenker og vedlegg i e-post. Brukerne er også opplærte til hvordan de selv kan sjekke om lenker og vedlegg er trygge via nettsiden *virustotal.com*.

Respondentene anerkjenner at enkelte subkulturer og demografier innad i selskapet er mindre kompetent til å bruke IKT-verktøy og at også interessen for sikkerhet er varierende. Spesielt blant de som nærmer seg pensjonistalder er det en del som ikke er like vant med datamaskiner, som de yngre brukerne. IT-sikkerhetssjef B sier at noen ganger kan en oppleve en reell frustrasjon over enkelte ansattes bevissthet og IKT-ferdigheter, men at da blir nærmeste leder involvert for å sørge for at vedkommende får den opplæringen han har rett på. *«Brukeren har fått tildelt et verktøy, da må han læres opp til å bruke det, istedenfor at vi bare tror at alt er deres ansvar hele tiden.»*

5.4.2 Øvelser

Nettselskap A har utført egne øvelser på phishing der de selv sender ut en falsk e-post til alle ansatte, der de ansatte blir bedt om å oppgi brukernavn og passord, for å deretter registrere hvor mange det er som lar seg lure og offentliggjør resultatet internt. Beredskapsøvelser brukes i selskapene til å lære, og oppdatere ROS-analyser, tekniske barrierer, rutiner og testing av planer. I nettselskap A er det stort sett bare skrivebordsøvelser som gjøres, men IKT-sikkerhetskoordinator forteller at disse er nyttige, og fører ofte til justering av planer og prosedyrer. I nettselskap B og C har de i tillegg til skrivebordsøvelser, gjennomført skarpe øvelser med mer sjeldne scenario.

CISO B hevder at sammenlignet med HMS-relaterte beredskapsøvelser om værforhold og lignende, har det tradisjonelt vært lite bruk av beredskapsøvelser relatert til IKT og cybersikkerhet. Dette er imidlertid i ferd med å snu, og det er planlagt flere øvelser relatert til dette. Respondentene trekker frem beredskapsøvelser som en god måte å oppnå mer bevissthet og læring. Øvelsene resulterer ofte i nye tiltak og barrierer, som eksempelvis mer opplæring. Emnene i øvelsene er basert på egne ROS-analyser og hendelser i samfunnet rundt seg. Øvelsene er viktige for kontinuerlig læring og forbedring og gir blant annet viktig tilbakemelding til risikovurderinger og kompetanseopplæringsbehov.

5.4.3 Rapportering

Respondentene hevder det er god kultur for rapportering av feil og avvik, der det er lav terskel for å si ifra. IKT-sikkerhetskoordinator A sier at de ansatte er flinke til å si ifra om mistenkelige forhold. Han underbygger dette med at ansatte hyppig sier ifra om forhold som at «*mobilen oppfører seg rart*» etter å ha vært på ferie i Kina. CISO B mener at selv om rapporteringskulturen knyttet til avvik er god, bør de samtidig jobbe videre med å gjøre kulturen bedre. Med dette henviser han til at terskelen er nok varierende for enkelte til å si ifra, og noen vil nok føle at de svikter en kollega om de rapporterer inn noe.

Nøkkelen til en god rapporteringskultur er, ifølge IKT-sikkerhetskoordinator A, at brukere føler de blir hørt og at det blir gjort noe med det som rapporteres inn. Han sier også at det ikke må være noen fryktkultur der en sanksjoneres om en har gjort feil og at gulrot er mer effektivt enn pisk. Han illustrerer dette med et eksempel på premiering av ansatte som rapporterte inn kritikkverdige personverns forhold i forbindelse med implementering av EUs nye personvernregler (GDPR). I en periode praktiserte selskapet «Månedens GDPR-medarbeider» der navn, bilde og en artikkel om en medarbeider ble publisert om personer som hadde

rapportert inn forhold som ikke var i henhold til personvernregelverket for å premiere vedkommende. Avviksrapportering er en viktig kilde til læring i nettselskapene og en måte å overvåke sikkerheten. CISO B hevder at siden de er så få som arbeider med sikkerhet kan de umulig se alt selv, derfor er avviksrapportering verdifullt. IT-sjef C sier at han mistenker at nettselskapets rutiner for rapportering kunne vært bedre kjent blant de ansatte.

5.4.4 Regler, rutiner og prosedyrer

Alle ansatte har en rekke regler, rutiner og prosedyrer som de er forpliktet til å sette seg inn i relatert til cybersikkerhet. Dette handler blant annet om hvordan en skal forholde seg til sensitiv informasjon, og e-post sikkerhet. IT-sjef C sier at ved ansettelse må de ansatte skrive under på en taushetserklæring, og i den forbindelse blir det også gitt eksempler på hva som er å anse som sensitiv informasjon. IKT-sikkerhetskoordinator A sier at regler og prosedyrer kan være en effektiv barriere så lenge de blir fulgt, men det vil alltids være en mulighet for å omgå denne typen barrierer. Beredskapskoordinator A sier at regler og rutiner fint kan fungere som barrierer, og henviser til rutinen om at dersom en er usikker på om innholdet i en e-post er trygt, skal denne videresendes til IT-avdelingen. Slike barrierer øker bevisstheten til brukeren, samt gir nettselskapet en mulighet for å skaffe bedre oversikt over omfanget av hendelser, slik at de igjen kan utvikle bedre barrierer.

IT-sikkerhetssjef B sier at de har en tydelig IT-instruks som de ansatte skal sette seg inn i, men at en selvsagt ikke har noen garantier for at dette etterleves i en hektisk hverdag. IKT-sikkerhetskoordinator A sier at de har noen overordnete regler som gjelder for alle, også noen spesifikke regler for enkelte avdelinger. Han sier det er vanskelig å finne et felles regelsett som passer for alle. Han mener det er meget utfordrende å bevisstgjøre de ansatte om hvilke regler det er som gjelder, og at det er en krevende prosess ettersom det stadig kommer nye oppdateringer som gjør at ansatte må vedlikeholde kunnskapen sin om hvilke regelsett som er gjeldende.

En rutine som beskrives av IKT-sikkerhetskoordinator A er å gjennomføre bakgrunnssjekk av personell som skal ha tilgang til enkelte kritiske kraftanlegg. Dette er et krav fra beredskapsforskriften om at det skal gjennomføres en fullstendig bakgrunnssjekk inkludert kreditthistorikk før personer kan få lov å få tilgang til enkelte typer anlegg. *«… en kan jo diskutere hvorvidt det er relevant å gjennomføre en kredittsjekk, men det er i alle fall noe vi er pålagt å gjøre».*

6. Diskusjon

I dette kapittelet vil resultatene fra intervjuene drøftes opp mot det teoretiske rammeverket presentert i teorikapittelet. Kapittelet er delt inn etter forskningsspørsmålene. Avslutningsvis vil problemstillingen besvares.

6.1 Hvordan bruker nettselskapene ikke-tekniske barrierer, og hvilken funksjon har barrierene i nettselskapenes cybersikkerhet?

I denne delen vil nettselskapenes ikke-tekniske barrierer presenteres, og det vil redegjøres for hvilken funksjon de ikke-tekniske barrierene har i nettselskapenes cybersikkerhetsarbeid. I dette ligger det også å redegjøre for hva som er bakgrunnen for valg av barrierer, og hvorfor det er behov for barrierer. Nettselskapenes erfaring med ROS-analyser er derfor også inkludert ettersom dette er et verktøy for valg av barrierer og sammensetting av risikovurdering.

6.1.1 Hvorfor barrierer?

Innen risikostyring er barrierer viktige styringsvariabler (Aven et al., 2004). Risikostyring defineres som «*alle tiltak og aktiviteter som gjøres for å styre risiko*» (Aven, 2007, s.13). Dette inkluderer både å kartlegge og få innsikt i risiko, samt gjøre tiltak for å styre og kontrollere den (Lunde, 2014). Risikostyring handler om å oppnå en balanse mellom det å skape verdier og unngå ulykker, skader og tap (Aven, 2007). Nettselskapene har ansvar for å drifte og vedlikeholde strømnettet, og i dette arbeidet er de ansatte avhengige av brukervennlige IKT-tjenester i hverdagen**.** Nettselskapene eksponeres derfor for risiko, og risikostyringsprosessen handler om å styre denne risikoen på et akseptabelt nivå. I dette arbeidet er iverksetting og vedlikehold av barrierer sentralt (Lunde, 2014). Ved å iverksette hensiktsmessige barrierer for de identifiserte uønskete hendelsene, vil den totale risikoen som nettselskapene omgir seg med reduseres.

6.1.2 Risikovurdering

En forutsetning for å drive risikostyring er å sørge for at en har innsikt i hvilken risiko en står ovenfor, samt risikoens grad av styrbarhet (Aven, 2007). En kan i dette arbeidet benytte ulike former for risikoanalyser for å kartlegge og beskrive virksomhetens risikobilde, for å gi virksomheten et beslutningsunderlag for valg av løsninger og tiltak i risikostyringen (Lunde,

2014). For å gjennomføre risikovurderinger trenger nettselskapene kunnskap om tre hovedforhold: verdier, trusler og sårbarheter. Til sammen utgjør de trefaktormodellen (Engen et al., 2016).

Før nettselskapene kan danne barrierer, må de foreta en vurdering av hvilke verdier de ønsker å beskytte. Cybersikkerhetsbegrepet kan defineres som «*alt som er sårbart via IKT*» (NOU, 2015). Nettselskapene ønsker derfor å beskytte IKT-systemene i seg selv, og informasjonen som lagres på dem for å sikre produksjonsprosesser som spesielt strømforsyningen, som er avhengig av IKT for å fungere. I tillegg nevner respondentene at de ønsker å beskytte nettselskapets verdier og miljø som kan rammes dersom IKT og strømforsyning blir utsatt for en uønsket IT-hendelse. Dette inkluderer blant annet å beskytte de ansatte som bruker IKT, kundene som er avhengig av strømforsyning, samt nettselskapenes økonomi og omdømme.

Spesielt informasjonssikkerhet er en viktig del av nettselskapenes cybersikkerhet. Ettersom mye informasjon lagres digitalt, eller kan ende opp med å lagres digitalt, er det viktig for nettselskapene at de ansatte har en god forståelse av informasjonens verdi. I alle nettselskapene trekker respondentene frem at det er problematisk å danne en klar forståelse for hva det er som utgjør både sensitiv og kraftsensitiv informasjon. To av nettselskapene er i en prosess der det gjennomføres et større prosjekt for klassifisering av informasjon. Dette kan sees på som en form for verdivurdering for å kartlegge hvilken informasjon som er beskyttelsesverdig. Resultatene fra intervjuene viser at det er relativt uavklart for nettselskapene nøyaktig hvilken informasjon som skal beskyttes, og hvilken som ikke skal beskyttes. Dette medfører at det også er varierende oppfattelser blant de ansatte om hva som er beskyttelsesverdig informasjon, noe som utgjør en risiko for at sensitiv informasjon lastes opp på feil plasser. CISO B hevder at dette er et symptom på at virksomheten tidligere ikke har hatt en klar skala på informasjon i henhold til konfidensialitet, integritet og tilgjengelighet.

Potensielle trusler kan være andre stater, kriminelle grupperinger, enslige amatør-hackere, eller ikke-målrettet skadevare som spres over internett. Respondentene henviser spesielt til Russland og Kina. IT-sikkerhetssjef B sier at de følger med på myndigheter som PST, Kripos, NSM og Etterretningstjenesten sine vurderinger, som hevder at kraftbransjen er spesielt utsatt for etterretningsvirksomhet. Dette er vurderinger som nettselskapet tar innover seg, og som påvirker deres egne vurderinger. Litteratur om risikostyring i møte med intenderte angrep, henviser ofte til at risiko knyttet til ondsinnete handlinger bestemmes av en vurdering av trusselaktørenes intensjon og kapasitet (Engen et al., 2016). IT-sikkerhetssjef B sier at dersom en aktør har ubegrenset med tid og ressurser, kan de med høy arbeidsinnsats forsere barrierer.

På bakgrunn av dette hevder han at det er nødvendig med andre mekanismer til å identifisere og oppdage unormal aktivitet, ettersom ingen barrierer vil kunne ha 100% sikkerhet. Cybersikkerhet omfatter imidlertid også hendelser forårsaket av ikke-intenderte hendelser, eller hendelser som i utgangspunktet er intenderte, men som ikke er målrettet mot en spesifikk virksomhet (NOU, 2015). Eksempler på førstnevnte er teknisk svikt og menneskelige feilhandlinger, mens ikke-målrettet skadevare som spres via internett eksemplifiserer sistnevnte. Begrepene intensjon og kapasitet fanger dermed bare til en viss grad opp karakteristikkene til potensielle trusler. På bakgrunn av dette må nettselskapenes bruk av barrierer innen cybersikkerhet ta hensyn til både tilsiktede og utilsiktede hendelser.

For å beskytte verdier mot ulike trusler må nettselskapene vurdere hvor de er sårbare. Sårbarhet er et aspekt av både risikobegrepet og cybersikkerhetsbegrepet (Aven, 2007, NOU, 2015). CISO B hevder de er meget bevisst på hvilke sårbarheter de har, og hvilke som kan utnyttes til angrep. Flere respondenter trekker frem e-post som eksempel på en sårbarhet som kan utnyttes til angrep. Mennesket blir også av flere omtalt som det svakeste leddet, og gjennom sosial manipulering kan menneskelige feilhandlinger utgjøre en risiko som kan medføre uønskete hendelser. Nettselskapene holder seg oppdatert på både sårbarheter og trusler via samarbeidspartnere som KraftCERT og Forum for informasjonssikkerhet i kraftforsyningen (FSK), samt offentlige myndigheter som NVE, PST, NSM. I tillegg gjøres det egne vurderinger, samt at nettselskapene følger med på hendelsene ellers i samfunnet. En potensiell sårbarhet for nettselskapene er den enkelte ansatte.

6.1.3 Bruk av ROS-analyser innen cybersikkerhet

For å sammenstille en risikovurdering basert på verdier, trusler og sårbarhet, benytter nettselskapene ROS-analyser. ROS-analyser skal identifisere hva som er viktige bidragsytere til risiko og beskrive effekten av ulike tiltak på risikoen (Aven, 2007). I intervjuene kommer det frem at ROS-analysene benyttes som et beslutningsunderlag for valg av barrierer i risikohåndteringen. I utgangspunktet skal alle nye IT-tjenester og systemendringer risikovurderes før de tas i bruk. IKT-sikkerhetskoordinator A sier at de også har egne ROS-analyser som benyttes for å kartlegge potensielle angrepsflater og sårbarheter i IKT-systemene, samt en beskrivelse av konsekvensen av disse mulige angrepene.

Selv om ROS-analysene blir sett på som et nyttig verktøy av nettselskapene, går det igjen i intervjuene at det er utfordrende å fastsette sannsynlighet for at uønskete hendelser skal oppstå. Tradisjonell risikomodellering møter betydelige utfordringer i møte med intenderte angrep,

ettersom det forutsetter kunnskap om aktørenes intensjoner, og kapasitet til å endre strategi i møte med ny informasjon (Engen et al., 2016, Jore & Njå, 2010). Respondentene antyder at en i mange tilfeller «*bare må bli enig om noe*» for å fastsette sannsynlighet, og at mesteparten av tiden går til å vurdere hva som er konsekvensene av ulike hendelser, og hvilke sårbarheter som eksisterer. ROS-analysene beskrives imidlertid som et godt verktøy for å få med potensielle hendelser en skal beskytte seg mot, og konsekvenser av ulike hendelser.

Respondentene viser til flere tilfeller der ROS-analyser blir benyttet som et beslutningsunderlag for valg av barrierer for å styrke cybersikkerheten. Dersom risiko havner utenfor risikoakseptkriteriene blir det ifølge respondentene stort sett satt bestemte tiltak med tidsfrister for når de skal være gjennomført. Her hevder imidlertid CISO B at deres virksomhet har forbedringspotensial, ettersom enkelte risikoanalyser ikke blir tilstrekkelig fulgt opp. Han peker også på at det i enkelte prosjekter ikke blir gjort risikovurderinger tidlig nok i prosessen. Dette medfører at en ikke har et bevisst forhold til hvilken informasjon nye system skal behandle, og dermed kan det også mangle barrierer som beskytter denne informasjonen. I nettselskap A sier imidlertid IKT-sikkerhetskoordinator A at ROS-analysene stort sett fører til risikoreduserende tiltak. IT-sjef C sier at prosessen ved å lage ROS-analyser har en verdi i seg selv, ettersom det fører til at en gjennom dialog med kollegaer får en bedre bevissthet om risiko. En kan dermed argumentere for at ROS-analyser kan fungere som en barriere i seg selv dersom den medfører at bevisstheten til de ansatte øker, og dermed virker preventivt mot uønskete hendelser. ROS-analyser er imidlertid først og fremst et verktøy for å bestemme barrierer, heller enn en barriere i seg selv.

Innen risikohåndtering vil flere av de risikoreduserende tiltakene som avdekkes i ROS-analysen være å forstå som barrierer ettersom de har som hensikt å forhindre at uønskete hendelser skal oppstå (Rosness et al., 2002). Flere av disse barrierene vil regnes som ikke-tekniske, eller myke barrierer. IT-sjef C henviser her til eksempler på at ROS-analyser har ført til at en har valgt å sette inn styrket opplæring som et risikoreduserende tiltak. Det er også vanlig ifølge respondentene å oppdatere regler, rutiner og prosedyrer som følge av ROS-analyser. I det følgende vil det redegjøres for hvilke ikke-tekniske barrierer nettselskapene benytter.

6.1.4 Hvilke ikke-tekniske barrierer benyttes, og hvilken funksjon har de?

ROS-analyser fører ofte til at barrierer blir iverksatt, eller at allerede eksisterende barrierer blir forbedret (Aven, 2007). CISO B hevder imidlertid at det i enkelte tilfeller ikke gjennomføres ROS-analyser, noe som kan tyde på at ikke alle barrierer nødvendigvis planlegges basert på en

risikovurdering. Det er imidlertid omfattende bruk av ikke-tekniske barrierer i nettselskapenes arbeid med cybersikkerhet. Reason (1997) hevder at myke barrierer omfatter en kombinasjon av mennesker og papirer, og eksemplifiserer dette med blant annet regler og prosedyrer, opplæring, trening og instrukser (Reason, 1997). Respondentene nevner en rekke sikkerhetsfunksjoner som kan kategoriseres som myke barrierer. Disse kan grupperes etter hvorvidt de er å anse som symbolske eller immaterielle (Hollnagel, 2008).

Symbolske barrierer

Hollnagel (2008) hevder at symbolske barrierer omfatter instrukser, prosedyrer, dialog, skilting, signaler, advarsler, tillatelser og lignende. Disse barrierene oppnår sin funksjon gjennom at de regulerer hvordan en skal handle, og gir informasjon for å oppnå korrekt sikkerhetsadferd (Hollnagel. 2008). Store deler av nettselskapenes opplæringstiltak innen informasjonssikkerhet og cybersikkerhet vil kunne kategoriseres som symbolske barrierer. De ansatte i nettselskapene har blant annet en IT-sikkerhetsinstruks som de er forpliktet til å følge. Dette er en symbolsk barriere ettersom at den er avhengig av at de den gjelder for forplikter seg til å følge den og forstår innholdet i den (Hollnagel, 2008). Dette er dermed barrierer som kan omgås dersom de ansatte ikke ønsker å følge instruksjonene, og nettselskapene mangler mulighet for å kontrollere manglende etterlevelse. Det samme kan sies om tiltak som er satt inn for å øke de ansattes bevissthet og kunnskap. Dette inkluderer blant annet E-læring, signering av taushetserklæring, informasjon via kanaler som intranett, møter, konferanser, foredrag og kurs. Dette er symbolske barrierer ettersom de ansatte må forstå, og til enhver tid huske innholdet for at de skal være effektive barrierer (Hollnagel, 2008). Dette gjelder også instruksen i nettselskap B der brukerne selv kan sjekke om mistenkelig e-post er legitim via nettsiden *virustotal.com.* Det eksisterer også en e-post-ordning i selskapene der en kan sende inn mistenkelige e-poster til IT-avdelingen.

Andre symbolske barrierer kan være bakgrunnssjekk av personell som skal ha tilgang til enkelte kraftanlegg. Dette gjennomføres for å forhindre at personer som utgjør en sikkerhetsrisiko basert på personlige karakteristikker som kreditthistorikk, ikke skal få tilgang til kritiske anlegg. Dette er en symbolsk barriere ettersom det er ingenting i seg selv med bakgrunnssjekken som hindrer personer med uønskete karakteristikker i å være til stede på kritiske anlegg. Effektiviteten til barrieren avhenger av at det faktisk blir foretatt en grundig bakgrunnssjekk, og at de gjennom andre barrierer og tiltak sørger for å forhindre personer som ikke er egnet tilgang. De symbolske barrierene har dermed en felles karakteristikk med at de mer eller mindre kan omgås av mennesker dersom de ønsker det.

Hollnagel (2008) hevder at en prosedyre også kan forstås som en symbolsk barriere ettersom det er en instruks for hvordan en skal handle, og at den bare fungerer gjennom at dens mening blir tolket og forstått korrekt (Hollnagel, 2008). En beredskapsplan, og øvelser på beredskapsplaner er også en form for instruks for hvordan en skal handle i en beredskapssituasjon. En kan derfor si at beredskapsplanverk, og nettselskapenes beredskapsøvelser er å anse som symbolske barrierer innenfor Hollnagels begrepsapparat. Her kan en også legge til phishing-øvelsen til nettselskap A, som hadde som hensikt å teste hvor mange ansatte som ble lurt av nettselskapets egen phishing-epost, og å øke bevisstheten om phishing. Dette er også en øvelse som har som funksjon å lære de ansatte hvordan en skal handle i en spesifikk situasjon.

Immaterielle barrierer

Hollnagel kategoriserer også enkelte myke barrierer som immaterielle. Dette er barrierer som ikke er fysisk til stede i situasjonen de skal anvendes i. Dette er barrierer som organisasjonen har pålagt systemet, men som ikke er fysisk, funksjonelt eller symbolsk til stede i systemet. De immaterielle barrierene avhenger dermed fullstendig av brukerens kunnskap for å oppnå dens funksjon (Hollnagel, 2008)

Hollnagel eksemplifiserer de immaterielle barrierene med lover og regler, etiske normer, sosialt press og selvbeherskelse. Dette er en type barrierer som består av kulturelle og organisatoriske forhold, og fungerer ofte som rammebetingelser for at andre barrierer skal fungere. For at en regel skal fungere må brukeren vite at regelen eksisterer, og inneha kunnskap og forståelse for regelens anvendelsesområde. I tillegg kan det også være avgjørende hvilken personlig etikk og selvbeherskelse brukeren har for hvorvidt hun vil ønske å handle i samsvar med regelen eller ikke. IKT-sikkerhetskoordinator A sier at en regel er en barriere som kan omgås, men dersom den blir fulgt kan den være veldig effektiv. Han sier imidlertid også at det er vanskelig å opplyse alle ansatte om hvilke regler det er som gjelder til enhver tid.

Immaterielle barrierer har mye til felles med elementer som inngår i en sikkerhetskultur. Reason (1997) hevder at en sikkerhetskultur blant annet består av produktet av individer og gruppers verdier, holdninger, kompetanse, og atferdsmønstre som viser forpliktelse og dyktighet i forhold til organisasjonens helse- og sikkerhetsprogrammer (Reason, 1997). En kan argumentere for at en god sikkerhetskultur totalt sett vil utgjøre en form for immateriell barriere, ettersom en sikkerhetskultur ikke er noe som fysisk eksisterer i seg selv. IT-sikkerhetssjef B

sier at arbeidet med en god sikkerhetskultur er en del av risikostyringsprosessen, og at dette arbeidet blant annet består av opplæring og undervisning.

Ettersom at mennesker har et betydelig ansvar for cybersikkerhet i hverdagen, kan kvaliteten på immaterielle barrierer være med å avgjøre hvordan de ansatte handler i arbeidshverdagen. Det er f.eks. regler som påbyr å kryptere sensitiv informasjon før det sendes over e-post. Det er også regler knyttet til passord, og hvilke IT-tjenester en kan benytte i arbeidshverdagen. I alle nettselskapene er det en aktuell problematikk at ansatte laster opp sensitiv informasjon på eksterne skytjenester som ikke er godkjent. Regler som forbyr enkelte handlinger, vil dermed kunne virke preventivt mot enkelte typer hendelser. De ansattes etikk vil også fungere som barrierer dersom dette motiverer ansatte til å være varsom med å dele sensitiv informasjon til personer som egentlig ikke trenger denne informasjonen. I nettselskap B har det vært problemer med at de ansatte stadig finner nye måter å benytte seg av programvare og IT-tjenester som ikke er godkjent («skyggetjenester»). Dette viser på den ene siden hvor lett det er å omgå en barriere som en regel, men samtidig også viktigheten av andre immaterielle barrierer som personlig etikk og selvbeherskelse i situasjoner der de tekniske barrierene ikke har klart å stenge tilgangen til alle skyggetjenester.

Hollnagel (2008) opererer med fire hovedkategorier av barrierer, men sier at barrierene også kan være en kombinasjon av flere typer, og det kan derfor være problematisk å kategorisere enkelte barrierer. I **Tabell 2** oppsummeres de ulike myke barrierene som ble nevnt av nettselskapene, og gruppert inn om hvorvidt de er å anse som symbolske eller immaterielle.

Symbolsk	**Immateriell**
Sikkerhetsmåned, konferanser, phishing-øvelse**,** beredskapsøvelser, e-læring, taushetserklæring, IT-sikkerhetsinstruks, bransjesamarbeid, e-post-ordning, kurs, bakgrunnssjekk og prosedyrer	Regler, sikkerhetskultur, etiske normer, selvbeherskelse og sosialt press

Tabell 2 Myke barrierers som identifiseres i nettselskapene.

6.1.5 Oppsummering: Ikke-tekniske barrierers rolle i risikostyring

ROS-analyser er et verktøy for å velge ikke-tekniske barrierer, men ifølge respondentene er det betydelige utfordringer med å fastsette risikonivå. I enkelte tilfeller er også risikovurderingene fraværende. Dette fører til at valg av barrierer ikke nødvendigvis alltid er risikobasert, ettersom det er problematisk å fastsette risikonivå i enkelte tilfeller. Myke barrierer har imidlertid en sentral rolle innen risikohåndteringen. Nettselskapenes sikkerhet består av en rekke myke og harde barrierer, og respondentene sier at kombinasjonen av tekniske og organisatoriske barrierer er viktig for god cybersikkerhet. IT-sikkerhetssjef B sier at barrierene deres er organisert etter prinsippet om forsvar-i-dybden, og utdyper at dette betyr at dersom en barriere svikter i å forebygge en trussel, skal en annen barriere demme opp. Alle nettselskapene har også som uttalt prinsipp at ingen barrierer alene kan være 100% sikre, og vil dermed alltid ha sårbarheter. Dette peker i retning av en forståelse lik Reason (1997) om forsvar-i-dybden som illustreres gjennom sveitserostmodellen gjennomgått i teorikapittelet.

Et funn i intervjuene er at myke barrierer brukes av nettselskapene i et samspill med tekniske barrierer, der myke barrierer ofte er nødvendige for å støtte opp om funksjonen til tekniske barrierer. Et eksempel på dette er kryptering av sensitiv informasjon før den sendes over e-post. I henhold til Reason (1997) sitt begrepsapparat kan en forstå selve krypteringsfunksjonen som en hard barriere. Uten myke barrierer som et regelverk som påbyr kryptering av sensitiv informasjon, samt barrierer som øker bevisstheten om regelen og risikoen ved å bryte den (f.eks. opplæring og informasjonskampanjer), så vil ikke denne harde barrieren være like pålitelig.

Hollnagel (2008) hevder at både symbolske og immaterielle barrierer har lav effektivitet, og kan enkelt omgås. Immaterielle barrierer bør derfor ikke benyttes som eneste barriere i sikkerhetskritiske operasjoner (Hollnagel, 2008). Nettselskapene har imidlertid et stort fokus på å bruke myke barrierer sammen med harde barrierer. Respondentene hevder likevel det er urealistisk å noen gang oppnå 100% menneskelig pålitelighet på blant annet phishing, men at de myke barrierene fungerer som sannsynlighetsreduserende tiltak. Kombinert med konsekvensreduserende barrierer og harde barrierer bidrar dermed myke barrierer med å redusere risikoen for uønskete cyberhendelser.

6.2 Hvilken betydning har nettselskapenes forståelse av menneskelige feilhandlinger for barrierestyring innen cybersikkerhet?

Alle respondentene sier at cybersikkerhet er et felles ansvar, og derfor jobber alle de ansatte i nettselskapene med cybersikkerhet. I gjennomgangen av nettselskapenes bruk av ikke-tekniske barrierer innen cybersikkerhet (**6.1**), kom det frem at mange av barrierene er iverksatt for å redusere risikoen for menneskelige feilhandlinger. Dette innebærer både å redusere antall feil, og redusere konsekvensene av de feilene som likevel forekommer. Feilene omfatter blant annet å trykke på phishing-lenker og videre oppgi brukernavn og passord, laste opp sensitiv informasjon på feil plasser, svake holdninger til passord, og bruk av skyggetjenester. Dette er feil som representerer en risiko for nettselskapene, og akkumulering av disse feilene kan i verste fall føre til at større hackerangrep lykkes.

Betegnelsen MTO brukes for å forklare samspillet mellom mennesker, teknologi og organisasjon. Hensikten er å undersøke hvordan menneskers fysiske, psykiske og sosiale forutsetninger samspiller med teknologi og organisatoriske forhold (Bento, 2001; Rollenhagen, 1997). Bento (2001) peker på at organisatoriske forhold legger føringer for hvorfor MTO-problemer forekommer, som f.eks. kommunikasjonsutfordringer, manglende opplæring og utfordrende arbeidsmiljø. Også Dekker (2006) og Reason (1997) knytter menneskelige feil opp mot karakteristikker ved selve det sosiotekniske-systemet eller organisasjonen, istedenfor at hver menneskelig eller aktiv feil sees på som en isolert årsak i seg selv til at ulykker oppstår. I det følgende vil det gjennomgås hvordan nettselskapenes forstår menneskelige feil, og hvordan dette påvirker deres valg av ikke-tekniske barrierer.

6.2.1 Nettselskapenes forståelse av menneskelige feilhandlinger

Respondentene fra nettselskapene ble alle spurt om hvorfor menneskelig feil forekommer. Flere av respondentene trakk frem at en kilde til feil kunne være en hektisk arbeidshverdag med tidspress, ønske om produktivitet, og en enklere hverdag. Dette kan ifølge Rasmussen (1997) og Reason (1997) ha innvirkninger på arbeidsplassens holdninger, normer og kultur, og kan bidra til å legge til rette for menneskelige feilhandlinger. Dekker bruker begrepet *«det lokale rasjonalitetsprinsippet»* om menneskelige feilhandlinger (Dekker, 2006). Mange handlinger gir mening i øyeblikket de blir begått, fordi de blir gjort av hensyn til andre målsettinger enn bare

sikkerhet (Dekker, 2006). Nettselskapene eksisterer ikke bare for å unngå uønskete cyberhendelser, men også for å drifte strømnettet og ivareta samfunnets behov for energi. Innad i nettselskapet vil de ansatte ha ulike stillingstitler, og bare et fåtall av disse vil ha et primært ansvar for sikkerhet.

IKT-sikkerhetskoordinator A hevder at det er problematisk at en del eksterne tjenester som *Office 365* oppfattes som mer brukervennlig, enn deres egne tjenester, og at dette kan medføre at brukere kan laste opp kraftsensitiv informasjon på eksterne skytjenester. Å laste opp kraftsensitiv informasjon i eksterne skytjenester er ansett som en menneskelig feil blant nettselskapene. Dette kan likevel være rasjonelt for brukerne forutsatt at de selv anser risikoen som akseptabel, og at de eksterne tjenestene gjør deres arbeidsdag enklere. En slik feil kan like gjerne forklares gjennom karakteristikker med nettselskapenes sosiotekniske-system som f.eks. manglende brukervennlighet i deres IT-tjenester, samt manglende forståelse av risiko blant de ansatte, heller enn at ansatte bevisst velger å gjøre risikofylte handlinger (Dekker, 2006; Rasmussen, 1997; Reason, 1997). Nødvendigheten av gode, brukervennlige tjenester er et gjennomgangstema i intervjuene, og respondentene mener de må tilrettelegge for brukerne. IT-sjef C sier at dersom noen oppgaver oppfattes som «et herk», så vil ikke brukerne gjøre det, og derfor blir ikke alltid sensitiv informasjon kryptert før det blir sent. To av respondentene sier at en må balansere sikkerheten med brukervennlighet, og at på grunn av problemer med brukervennlighet kan det oppstå menneskelige feil, slik som eksemplet med e-post-filteret som skulle være en barriere mot phishing-e-poster, men som ikke fungerte optimalt. Denne tekniske barrieren ble så fjernet, men et resultat av dette er at brukerne nå eksponeres for større risiko for phishing.

Respondentene trekker også frem flere andre eksempler på hvordan konflikterende målsettinger i nettselskapet kan resultere i nedprioritering av sikkerhet (Dekker, 2006, Rasmussen, 1997). Dette gjelder blant annet mottagelsen av informasjon via intranett. Flere av respondentene hevder at det publiseres for mye informasjon på intranett, da plattformen brukes til å formidle sikkerhetsinformasjon, men også andre tema som f.eks. arbeidsmiljø. Dette medfører at volumet av informasjon blir for stort til at de ansatte klarer å få med seg alt. I nettselskap A er det frivillig å abonnere på informasjonen om informasjonssikkerhet, noe som kan medføre at bare de som er mest interessert får med seg informasjonen. Det er naturlig at det innad i nettselskapene vil være ulik interesse for sikkerhet, når ikke alle arbeider like mye med sikkerhet i sin arbeidshverdag. Dette er forklaringer som kan peke i retning av Dekker (2006) sitt nye syn på menneskelig feil.

Flere av respondentene vektlegger de ansattes bevissthet om hva som utgjør sensitiv informasjon, og risikoforståelse som forklaringer på hvorfor feil forekommer. CISO B hevder at manglende forståelse av hva som utgjør kraftsensitiv informasjon er et symptom på at virksomheten har hatt mangelfull klassifisering og eksempler på hva slags informasjon som skal beskyttes å vise til. Dette er en forklaring som peker i retning av organisatoriske mangler, heller enn karakteristikker ved den enkelte ansatte. En kan argumentere for at dette er det som Reason (1997) omtaler som latente forhold. De fleste respondentene sier at opplæringen kan forbedres, og flere anser det som en av de viktigste grunnene til at de ansatte gjør feil. IT-sikkerhetssjef B sier at når man har gitt en ansatt et verktøy, må han få opplæring så han kan bruke det. Bento (2001) hevder at mangelfull opplæring kan bidra til MTO-problemer, og at det er nødvendig å vurdere hvorvidt opplæringsmetodene er samstemte med oppgaven som skal utføres. Manglende opplæring kan dermed være et latent forhold som øker sannsynligheten for aktive feilhandlinger (Reason, 1997)

Alle respondenter peker generelt på karakteristikker ved organisasjon og system, heller enn karakteristikker med de ansatte som forårsaker at de gjør feil. Nettselskapenes forståelse kan derfor tolkes som å ligge nærmere det nye synet på menneskelige feil, enn det gamle (Bad Apple-teori) (Dekker, 2006). Det er imidlertid også enkelte utsagn som peker i retning av Bad Apple-teori. IKT-sikkerhetskoordinator A sier at mangelfull opplæring antageligvis er den viktigste forklaringen på feilhandlinger, men han mener også at mange av feilene som begås skyldes «slurv» og «uforsiktighet», eller at enkelte ikke tenker seg godt nok om før de handler. Dette forklares ved ulike personlighetstyper hos de ansatte, som fører til at enkelte har større risikoaksept og føler mindre ansvar for sikkerhetsarbeid. Han antyder at enkelte på grunn av svake holdninger nærmest gjør feil med vilje. Dette peker i retning av Bad Apple-teori, ettersom feilene i seg selv brukes som forklaring på hvorfor de oppstår (Dekker, 2006).

6.2.2 Den menneskelige faktor i barrierestyring

Latente og systemiske forhold som blant annet mangelfull opplæring, hektisk arbeidshverdag og manglende brukervennlighet preger forklaringene til respondentene for hvorfor menneskelige feil oppstår. I kapittel **6.1** ble det presentert en rekke ikke-tekniske barrierer som brukes for å blant annet forhindre disse feilene. Flere utsagn tyder på at forståelsen av menneskelige feil peker i retning av «The New View». Dette gjenspeiles også i valgene av barrierer. Spesielt barrierer innenfor opplæring vektlegges av respondentene. IT-sjef C sier at det er vanskelig for vanlige brukere uten IKT-utdannelse å vite de teknologiske implikasjonene av handlingene deres. Bento (2001) hevder at opplæringen bør gi en innføring i hvilke

konsekvenser eventuelle feil kan forårsake. I nettselskap B arrangeres det jevnlig opplæring som tar utgangspunkt i hendelser som skjer ellers i samfunnet, som f.eks. cyberangrepet mot Hydro. Slik forstår brukerne hvilke konsekvenser som potensielt kan oppstå dersom det blir gjort feil. Samtidig sier flere av respondentene at truslene blir stadig mer sofistikerte, og at tidligere tiltak som å lære brukere å sjekke avsenderadresse nå ikke lenger er tilstrekkelig. Dette fører til at selv folk fra IT-avdelingen lar seg lure av phishing-lenker. Bare i nettselskap A har en hatt en øvelse som direkte tester alle ansatte i phishing, ved å selv sende ut en falsk e-post. Selv om nettselskapene har flere ulike tiltak i form av opplæring og informasjon om trusler til de ansatte, kan en likevel stille spørsmål om de ansatte har nok erfaring i å håndtere sofistikerte phishing-forsøk, når det sjeldent øves direkte på det. Dersom de ansatte skal håndtere en situasjon som sjeldent forekommer er det viktig at brukerne av teknologien får regelmessig oppdatert kunnskapene sine (Bento, 2001). Ettersom det er flere tekniske barrierer som fjerner det aller meste av phishing-forsøk og skadelige vedlegg før det når brukeren, er det også sjeldent at det er skadevare direkte på e-postene, noe som kan medføre begrenset erfaring for brukere til å håndtere phishing.

Selv om respondentene hevder opplæringen kan forbedres, er det likevel tydelig at opplæring har høy prioritering, og utgjør en vesentlig del av de ikke-tekniske barrierene innen cybersikkerhet. Alle nettselskapene deltar på sikkerhetsmåneden, som inkluderer både e-læring, og et generelt fokus på informasjon om cybersikkerhet. I tillegg bruker nettselskapene egne e-læringsplattformer til å lære opp de ansatte. Nettselskap B utmerker seg med spesielt mye fokus på undervisning, der de ansatte blant annet deles inn i grupper for å løse oppgaver. CISO B forsøker å invitere seg selv inn til de ulike avdelingene for å finne ut hva hver enkelt sliter med for å tilpasse undervisningen. Eksterne foredrag og konferanser fra f.eks. NVE og NSM brukes også til undervisning ved flere nettselskap. CISO B sier at ettersom de er så få ansatte i avdelingen for informasjonssikkerhet, er de avhengig av opplæring av ansatte i sikker bruk av IKT. IT-sikkerhetssjef B trekker frem eksemplet om å lage et ark med prosedyrer for hvordan en kan sjekke om mistenksomme e-poster er trygge. Brukerne er også opplærte til at de kan sende inn e-poster til IT-avdelingen dersom de er usikre. Det gjøres dermed mye preventivt arbeid som for å gjøre de ansatte bedre rustet til å ta rette valg i arbeidshverdagen. Opplæringsrutiner, prosedyrer, arbeidsmiljø, og ansvarsforhold vil være en del av nettselskapenes latente og systemiske forhold (Dekker, 2006; Reason, 1997)

Ettersom arbeidspress og en hektisk hverdag tillegges stor vekt av forklaringene på hvorfor menneskelig feil forekommer, kan det tenkes at det er begrenset hvor effektive ikke-tekniske

barrierer er. Preventive tiltak som regler og prosedyrer, opplæring og informasjonsdeling vil kunne gjøre de ansatte bedre rustet til å ta de rette avgjørelsene. Men dersom det er slik IT-sikkerhetssjef B sier at feilene først og fremst skyldes en hektisk hverdag, så vil det være begrenset hvor godt preventive ikke-tekniske barrierer vil fungere i situasjoner med høyt arbeidspress. Hollnagel (2008) sier at symbolske og immaterielle barrierer har lav effektivitet ettersom de ansatte fort glemmer de. Et nettselskap er et sosioteknisk system, der de ansatte er fullstendig avhengig av å bruke IKT i hverdagen for å utføre arbeidsoppgavene sine effektivt. Dette krever en viss frihet og brukervennlighet for den enkelte ansatte, men også konsekvensreduserende barrierer for å øke feiltoleransen (Rasmussen, 1997).

Ettersom respondentene går langt i å antyde at mennesker er et mulig svakt ledd, og at en aldri kan oppnå 100% menneskelig pålitelighet brukes det derfor konsekvensreduserende barrierer. Disse barrierene omfatter blant annet beredskapsøvelser og beredskapsplaner, i tillegg til funksjonelle og tekniske barrierer. Dette inkluderer å planlegge hvordan en skal agere i enkelte situasjoner, samt øve på ulike scenario. En kan også argumentere for at bevissthetssøkende tiltak vil virke preventivt i tilfeller der det i utgangspunktet er gjort en feil. Et eksempel på dette kan være at dersom de ansatte har god forståelse for hva som utgjør kraftsensitiv informasjon, vil det ikke være mulig å lese kraftsensitiv informasjon dersom uvedkommende klarer å få tilgang til en e-post konto, ettersom de ansatte uansett ikke vil ha sendt ukryptert kraftsensitiv informasjon over e-post.

Det er lite med nettselskapenes forståelse av menneskelige feil som minner om Bad Apple-teorien, og i intervjuene kom det heller ikke frem noen klare eksempler på barrierer som representerer et slikt syn. Nettselskapene har imidlertid et krav fra beredskapsforskriften at det skal gjennomføres full bakgrunnssjekk og kredittsjekk på personer som skal ha tilgang til enkelte anlegg (Beredskapsforskriften, 2012, §6-7). Det kan argumenteres for at en slik barriere ligger nærmere et syn som Bad Apple-teorien, ettersom en forsøker å unngå det man ser på som upålitelige mennesker fra systemet, istedenfor å endre systemet i seg selv (Dekker, 2006). Det er imidlertid vanskelig å knytte en slik barriere til nettselskapenes forståelse av menneskelig feil. IKT-sikkerhetskoordinator A sier *«… en kan jo diskutere hvorvidt det er relevant å gjennomføre en kredittsjekk, men det er i alle fall noe vi er pålagt å gjøre».*

Reason hevder at så lenge mennesker jobber i moderne teknologiske system, vil det alltid forekomme aktive feil, men en kan redusere sannsynligheten for at disse oppstår, og ikke minst konsekvensene av disse gjennom å forstå de latente forholdene (Reason, 1997). *"We cannot*

change the human condition, but we can change the conditions under which people work" Reason (1997, s. 15).

Resultatene fra intervjuene tyder på at nettselskapenes forståelse av menneskelig feil er preget av en oppfattelse av at det ligger en rekke faktorer bak en menneskelig feil, men at de fortsatt har en vei å gå for å tilpasse opplæringen og arbeidsdagen for å redusere feil.

6.3 Hvilken betydning har nettselskapenes kollektive bevissthet på ikke-tekniske barrieres pålitelighet innen cybersikkerhet?

Begrepet kollektiv bevissthet brukes om karakteristikker ved høypålitelige organisasjoner som kjennetegnes av å ha opprettholdt et høyt nivå av sikkerhet over lengre tid (Weick & Sutcliffe 2007; Weick et al., 1999). Weick et al., (1999) argumenterer for at denne tilstanden oppnås gjennom fem kognitive prosesser som til sammen utgjør den kollektive bevisstheten. I det følgende vil dette disse fem kognitive prosessene benyttes for å vurdere hvordan kollektiv bevissthet påvirker de ikke-tekniske barrierenes pålitelighet.

6.3.1 Nettselskapenes kollektive bevissthet

En HRO er alltid opptatt av at feil og overraskelser kan oppstå, og at en må benytte enhver feil til organisatorisk læring (Weick & Sutcliffe, 2007; Weick et al., 1999). Under intervjuene med nettselskapene kom det frem at nettselskapene opplevde lav forekomst av alvorlige uønskete hendelser. Respondentene var imidlertid veldig opptatte av å trekke frem mindre alvorlige feil, mulige risikofylte handlinger, samt forhold de mente var kritikkverdige, som for eksempel manglende forståelse av hva som utgjør kraftsensitiv informasjon. Ser en bort ifra kryptovirusene som to av nettselskapene ble utsatt for, har ikke phishing-forsøkene medført noen negative konsekvenser. Nettselskapene er likevel meget opptatt av de feilene som fortsatt gjøres i henhold til tvilsomme e-poster, ettersom dette medfører en risiko for at fremtidige angrep kan lykkes. Dette ser man ettersom flere av barrierene som benyttes har som sin primære funksjon å forhindre menneskelige feil.

En HRO som er opptatt av feil, er opptatt av noe den sjeldent opplever. For å lære av feil må den derfor utvide læringsmulighetene sine, gjennom blant annet å analysere nesten-hendelser (Weick & Sutcliffe, 2007). Mange av hendelsene som respondentene trekker frem, er ikke uønskete hendelser som hadde negative konsekvenser, og hendelsene kan dermed kategoriseres

som nesten-hendelser. Disse hendelsene blir likevel poengtert av respondentene som å være symptomer på at systemet ikke er så pålitelig som de ønsker, og viser at de ser potensialet for ulykker i systemet (Weick & Sutcliffe, 2007). Et annet eksempel på at nettselskapene utvider læringsmulighetene sine er at IT-sikkerhetssjef B bruker andre uønskede hendelser ellers i samfunnet i undervisningen. Disse hendelsene benyttes for å lære hvordan en kan unngå slike hendelser selv. Dette er et eksempel på at nettselskapet er opptatt av feil, og utvider læringsmulighetene sine i fravær av egne hendelser.

En HRO oppfordrer til, og belønner rapportering av feil (Weick & Sutcliffe, 2007; Weick et al., 1999). Nettselskapene hevder de de har en god kultur for rapportering av avvik og feil. IKT-sikkerhetskoordinator A sier de ansatte er flinke til å si ifra om mistenkelige forhold, og at det er lav terskel for å si ifra. I nettselskap A har man et eksempel på at rapportering av avvik i forbindelse med GDPR ble belønnet med hederlig omtale av «Månedens GDPR-medarbeider». Dette er altså en belønning av en medarbeider som har utmerket seg spesielt positivt med sin rapportering, samt et tiltak som kan stimulere andre til å rapportere. Respondentene vektlegger at de ikke vil ha en fryktkultur: rapporteringen skal føles trygg og enkel, og de ansatte skal føle at de blir hørt. I to nettselskaper sier respondenter at de tror de fortsatt har en vei å gå når det kommer til rapporteringskultur ettersom terskelen for å rapportere er varierende, og at rutinene rundt rapportering ikke er godt nok kjent. For å skape en rapporterende kultur bør rapporteringssystemet være brukervennlig og tillitsfullt, om systemet er tidskrevende og ikke oppleves som nyttig kan det skape rapporteringsvegring (Reason, 1997). I nettselskap C har man et eksempel på en bruker som trykket på en phishing-lenke og ga fra seg både brukernavn og passord, for å så rapportere inn dette. Hvis dette er et representativt tilfelle, kan det tyde på en rapporteringskultur der det fra de ansattes side oppleves som trygt å melde ifra om egne feil. En god rapporteringskultur vil være et viktig datagrunnlag for å overvåke barrierenes ytelse, og overvåking av sikkerhetsnivået (Reason, 1997).

Personell i alle organisasjoner som håndterer komplekse oppgaver gjør forenklete tolkninger i arbeidshverdagen i gitte situasjoner (Weick & Sutcliffe, 2007; Weick et al., 1999). Dette er en vanlig karakteristikk i de fleste organisasjoner, men disse forenklingene kan være potensielt farlig for en HRO, ettersom det kan medføre at vital informasjon ignoreres (Weick & Sutcliffe,2007; Weick et al., 1999). I en HRO er det derfor motstand mot forenklete fortolkninger, og det eksisterer heller en form for innebygd skepsis som medfører at operasjoner, rutiner og prosedyrer kontrolleres og møtes med skepsis. IT-sikkerhetssjef B sier at en ikke må se seg blind på fravær av uønskete hendelser. *«… fravær av uønskete hendelser*

og FLAKS er ikke noen god styringsparameter …». Han gjentar flere ganger at det er grunn til å tro at det eksisterer mørketall for feil som gjøres og at de derfor må jobbe med kontinuerlig forbedring, og at summen av barrierer aldri vil kunne gi 100% sikkerhet. Det kan være fristende å konkludere med at en har et tilstrekkelig sikkerhetsnivå så lenge en har fravær av hendelser, men en HRO vet at de opererer innenfor et komplekst system, der det er iboende potensiale for feil og overraskelser (Weick et al., 1999). Alle respondentene er imidlertid åpen for at større hackerangrep som angrepet i Ukraina utgjør en reell risiko mot deres virksomhet. Westrum (1988) argumenterer for at organisasjoner som er villig til å agere på spesifikke trusler, også er organisasjoner som er villige til å tenke på disse truslene. Nettselskapenes risikostyring av cybersikkerhet er i stor grad basert på å unngå sofistikerte cyberangrep, selv om slike angrep ikke har skjedd i Norge før. Dette peker i retning av at det er en motstand mot forenkling samt en forpliktelse til resiliens (Weick et al.,1999; Westrum, 1988).

Respondentene er opptatt av at cybersikkerhet er et felles ansvar, samtidig sier flere av respondentene at det ikke er alle som føler eierskap til dette ansvaret. Dette er i så fall en forenklet forståelse av egen rolle i nettselskapets cybersikkerhetsarbeid. Nettselskapene fokuserer i stor grad på opplæringstiltak med hensikt om å øke de ansattes bevissthet om cybersikkerhet. Dette er tiltak som gjør at de ansatte i større grad forstår at også de har en rolle i cybersikkerhetsarbeidet. Weick et al. (1999) hevder at en måte å oppnå redundans på i en HRO er gjennom skeptisisme som fører til en motstand mot forenklete fortolkninger, og at dette kan oppnås gjennom at det er rom for diskusjon, uenighet, tvil, skepsis for egen praksis, og flere observasjoner og synspunkt (Weick et al.,1999). CISO B sier at selv om han kommer til å anbefale at nettselskapet skal delta på sikkerhetsmåneden og gjennomføre E-læring, er han selv skeptisk til effekten av E-læring. Han sier at E-læring fungerer for de som er interessert og forstår innholdet, men at andre bare klikker seg raskt igjennom innholdet og glemmer budskapet. Derfor kompensere han med å også gjøre annen form for opplæring, som innebærer større grad av dialog med enkeltpersoner. Denne formen for skepsis kan gjøre at nettselskapet oppnår redundans i form av flere opplæringstiltak, enn de ville hatt med en forenklet fortolkning av opplæringens effekt. På den annen side sier flere av respondentene at de mistenker at opplæringen er for standardisert, og at den ikke fanger opp de som trenger mest opplæring. Dette tyder på den ene siden at respondentene har en motstand mot forenkling og er opptatte av feil, men på den annen side gjenspeiles ikke dette helt i opplæringsrutinene, ettersom denne nettopp er standardisert og ikke nødvendigvis tilpasset den enkelte ansatte.

I **6.2** ble det argumentert for at nettselskapenes forståelse av menneskelig feil peker i retning av Dekker (2006) sitt nye syn på menneskelig feil. For å unngå menneskelige feil, må man forstå hvorfor de oppstår. En forenklet forståelse av menneskelig feil ville bygget på det gamle synet på menneskelig feil som forklarer menneskelig feil som at feilhandlingene begås i et vakuum. Ettersom respondentene i stor grad forklarte feilene gjennom latente forhold, eller karakteristikker ved nettselskapene som system, kan dette tyde på at det er en motstand mot forenkling, samt et fokus på feil.

For at nettselskapenes barrierer skal være effektive, må en vite hvilke verdier en må beskytte. Informasjonssikkerhet er en vesentlig del av cybersikkerhet, og i alle nettselskap er det problemer med å forstå hva som utgjør kraftsensitiv informasjon. Nøkkelen ved operasjonell sensitivitet er å være følsom for hva som faktisk skjer i selve operasjonen og inneha oppmerksomhet ovenfor arbeidet som foregår i den skarpe enden (Weick et al., 1999). Ettersom noen ansatte mangler en klar forståelse av hva som utgjør kraftsensitiv informasjon, vil de også kunne mangle situasjonsforståelse ved håndtering av sensitiv informasjon. Dette peker i retning av at det er en manglende operasjonssensitivitet, manglende fokus på feil, og en forenklet forståelse av informasjonens verdi.

Det er en aktiv bruk av ROS-analyser i nettselskapene, men i nettselskap B er det eksempler på at ROS-analyser ender opp i en skuff, eller ikke blir tilstrekkelig fulgt opp. I to av nettselskapene er det også knyttet utfordringer til manglende kommunikasjon om risiko. Dårlig risikokommunikasjon og manglende tiltaksoppfølging kan medføre at barrierer ikke blir tilstrekkelig iverksatt eller overvåket. Dette er i så fall manglende bevissthet om både trusler og barrierer, som er et symptom på manglende situasjonsforståelse, og fokus på feil (Weick et al., 1999). I nettselskap B er det også prosjekter som utføres uten at det blir gjort risikovurderinger i startfasen, noe som gjør at sikkerhet ikke blir ivaretatt tidlig nok i prosjektet og som kan medføre manglende barrierer. Dette er også eksempler som peker i retning av manglende fokus på feil og manglende operasjonssensitivitet. Hvis ROS-analyser ikke blir gjort hyppig nok, eller at funnene som blir avdekket ikke blir tilstrekkelig fulgt opp, kan det tenkes at dette medfører manglende overvåking av barrierenes ytelse, samt manglende etablering av barrierer.

Forpliktelse til resiliens innebærer å forberede seg på å ha kapasitet til å håndtere overraskelser og farer (Weick & Sutcliffe, 2007; Weick et al., 1999). Selv om nettselskapene ønsker å unngå feil og uønskete hendelser, gjøres det også beredskapstiltak for å øve på hvordan en skal håndtere hendelser som likevel har oppstått. I alle nettselskapene gjøres det beredskapsøvelser relatert til cyberhendelser, men CISO B sier at det sammenlignet med HMS-øvelser, så har det

vært lite øvelser på cyberhendelser. Dette er imidlertid i ferd med å snu, og nettselskapene sier at de i større grad benytter seg av slike øvelser nå, og at beredskap er en prioritert oppgave. For at øvelsene skal fungere må en imidlertid ha rutiner for å evaluere øvelsene. Respondentene sier at evalueringen av øvelsene fører til at en oppdaterer rutiner og stadig finner måter å forbedre beredskapen på og oppdatere risikoanalyser. Dette kan dermed peke i retning av en forpliktelse til resiliens, og motstand mot forenkling. Beredskapsplaner og rutiner for hendelseshåndtering er også viktig med tanke på å redusere konsekvensen av eventuelle cyberangrep. Å ha resiliens innebærer å tåle at det forekommer menneskelige feil, uten at dette får alvorlige konsekvenser (Weick & Sutcliffe, 2007; Weick et al., 1999).

Nettselskapene beskriver en e-post-ordning som går ut på at dersom brukeren er i tvil om det er trygt å åpne en e-post, skal en videresende den til IT-avdelingen. Dette vitner om en forpliktelse til resiliens, og en desentralisert struktur som medfører at de med best kompetanse tar avgjørelser (Weick et al., 1999). Weick et al., (1999) hevder at en desentralisert struktur åpner opp for at de med relevant ekspertise skal ta sentrale avgjørelser. Respondentene viser til eksempler på at under utarbeidelsen av ROS-analyser deltar relevante fagfolk i utarbeidelsen av analysene, og at det tildeles eiere av risikoen og for gjennomføring av risikoreduserende tiltak**.** IT-sjef C sier at ROS-analyser alltid har en verdi ettersom sentrale fagfolk sitter sammen og diskuterer løsninger. CISO B sier at ledelsen er meget opptatt av arbeidet med cybersikkerhet og at deres avdeling har fått innpass hos konsernledelsen, som gjør at de kan påvirke beslutningsprosessene. Dette er eksempler som peker i retning av en desentralisert struktur med respekt for ekspertise (Weick et al., 1999). CISO B trekker imidlertid også frem eksempler på at en desentralisert struktur kan ha sine svakheter. Han hevder at det gjennomføres mange risikovurderinger, men at det mangler et system for å kommunisere disse til resten av organisasjonen. Ettersom nettselskapene forteller om få uønskede hendelser, er det vanskelig å vite hvordan nettselskapene vil agere under en større hendelse. I nettselskap B benyttes det beredskapsøvelser der en kartlegger rutiner for hvem som skal være med i hendelseshåndtering, og det arbeides med å sette sammen et responsteam.

Aven & Krohn (2013) hevder at de fem prinsippene som utgjør den kollektive bevisstheten er med å forklare høypålitelige organisasjoner (HRO) sin suksess. Disse prinsippene kan dermed brukes innen risikostyring, samt for å håndtere uforutsette hendelser og andre overraskelser (Aven & Krohn, 2013). Det er vanskelig å bevise hvorvidt de fem karakteristikkene er nøkkelen til pålitelighet, eller om det er andre forhold som gjør at nettselskapene opplever såpass få alvorlige hendelser. En kan i varierende grad observere karakteristikker av kollektiv bevissthet

i nettselskapenes risikostyring innen cybersikkerhet. Nettselskapene har et stort fokus på feil og svake signaler, noe som medfører at det etableres suksessive lag med barrierer. Selv om det er grunn til å forvente mørketall om uønskete cyberhendelser, leser vi ikke om store hackerangrep i media, og påliteligheten til kraftforsyningen er god. Dette kan tyde på at barrierene fungerer, og at det er flere eksempler på at ikke-tekniske barrierer er viktige i nettselskapenes cybersikkerhet.

Risikobildet er i konstant endring, og truslene blir stadig mer sofistikert. Det er dermed viktig med bevissthet om både trusler og barrierer. I **6.1** så man at myke barrierer kan omgås dersom de ansatte ikke har god nok bevissthet rundt barrierens funksjon (Hollnagel, 2008). Enkelte funn tilsier at det er manglende risikoforståelse, samt manglende verdibevissthet ettersom det er problemer med å oppnå bevissthet rundt hva som utgjør kraftsensitiv informasjon. Dersom det er manglende bevissthet om hvilke verdier barrierene skal beskytte, kan dette også påvirke barrierenes pålitelighet. Forenklete fortolkninger kan også medføre at barrierene som velges ikke blir kritisk vurdert i stor nok grad. Flere av respondentene sier at opplæringen ikke fanger opp alle ansatte og at opplæringstiltakene generelt kan forbedres, som kan tyde på en motstand mot denne typen forenkling. Dette viser at kollektiv bevissthet påvirker både valg av barrierer og overvåkingen av barrierenes ytelsesnivå, noe som igjen kan påvirke påliteligheten til barrierene.

6.4 Avsluttende drøfting og svar på problemstilling

Denne studien har tatt utgangspunkt i problemstillingen: *Hvordan forstår nettselskaper betydningen av ikke-tekniske barrierer innen cybersikkerhet?*

For å svare på problemstillingen har nettselskapenes erfaringer med ROS-analyser og ikke-tekniske barrierer blitt diskutert. Resultatene viser at det er omfattende bruk av ikke-tekniske barrierer, og at alle respondentene vektlegger organisatoriske og menneskelige forhold i tillegg til de tekniske. ROS-analyser fremstilles som et nyttig verktøy for å velge både tekniske og ikke-tekniske barrierer, men det er likevel flere eksempler på at kvaliteten på risikostyringsprosessen kunne vært bedre. De ikke-tekniske barrierene er spesielt viktige innenfor opplæring og sikkerhetsbevissthet. I tillegg er det flere eksempler på at regler, rutiner og prosedyrer er viktige for å støtte opp om funksjonaliteten til de tekniske barrierene.

Nettselskapenes forståelse av menneskelige feilhandlinger peker i retning av Dekker (2006) sitt nye syn på menneskelig feil, og dette ser man også i at flere av de ikke-tekniske barrierene har som sin primære funksjon å begrense menneskelige feilhandlinger gjennom blant annet opplæring. En kan likevel stille spørsmål ved om nettselskapenes ikke-tekniske barrierer innenfor opplæring tar høyde for hvor forskjellige mennesker er, og at opplæringen framstår som i overkant standardisert. De fem kognitive prosessene som ifølge Weick et al., (1999) utgjør kollektiv bevissthet observeres i varierende grad hos nettselskapene. Dette kan tyde på at nettselskapene er årvåkne i møte med cybertrusler, og at dette påvirker påliteligheten til de ikke-tekniske barrierene.

Samtidig har denne studien demonstrert begrensningene til ikke-tekniske barrierer. Resultatene støtter opp om Hollnagel (2008) sin påstand om at immaterielle og symbolske barrierer ofte har lav effektivitet ettersom brukerne kan simpelthen velge å omgå barrierene. Dekker (2006) sier imidlertid gjennom «det lokale rasjonalitetsprinsippet» at de fleste handlinger gir mening når de blir begått. Selv om brukere velger å omgå en myk barriere gjennom f.eks. å bryte en regel, så kan det være rasjonelt fra brukerens ståsted å ikke følge denne, av hensyn til produktivitet og effektivitet (Rasmussen, 1997; Reason, 1997). Dette viser på den ene siden hvor ineffektive myke barrierer er, men på den annen side hvorfor cybersikkerhet må analyseres gjennom et helhetlig sosioteknisk perspektiv som fokuserer på samspillet mellom mennesker, teknologi og organisasjon. For at barrierene skal fungere må de imøtekomme både menneskelige og organisatoriske behov (Albrechtsen & Hovden, 2011). Dette gjelder både tekniske og ikke-tekniske barrierer, og begge typer barrierer kan være ineffektive dersom de ikke tar hensyn til det sosiotekniske-systemet som mennesker og teknologi opererer i. Dersom de ansatte opererer i et krevende arbeidsmiljø, vil de være dårligere rustet til å utøve korrekt sikkerhetsadferd (Bento, 2001; Rasmussen, 1997).

Nettselskapene har flere målsetninger enn bare god cybersikkerhet, og flere av målene konflikter med hverandre. IT-sikkerhetssjef B oppsummerer dette med at de ønsker å ha både brukervennlighet og sikkerhet, og de må oppnå en balanse mellom de to. En effektiv HRO klarer å balansere disse motstridende perspektivene, og Weick et al. (1999) sitt begrep om kollektiv bevissthet kan fungere som en veileder for å oppnå denne kapasiteten. Spesielt bevisstheten til de ansatte om risiko og trusler er vesentlig. Dersom de ansatte ikke vet hvilke verdier det er som skal beskyttes, vil de heller ikke være klar over sårbarheter eller hva som kan være potensielle trusler. De ansattes kollektive bevissthet vil dermed påvirke påliteligheten til

barrierer, både tekniske og ikke-tekniske. For å oppnå denne bevisstheten bruker nettselskapene et mangfold av ikke-tekniske barrierer som fungerer i et samspill med de tekniske.

7. Konklusjon og forslag til videre forskning

7.1 Konklusjon

Denne studien har undersøkt problemstillingen: *Hvordan forstår nettselskaper betydningen av ikke-tekniske barrierer innen cybersikkerhet?*

Sikkerhetsledere i nettselskap har derfor blitt intervjuet om deres erfaringer med ROS-analyser og ikke-tekniske barrierer. Resultatene viser at nettselskapene bruker en rekke ulike ikke-tekniske barrierer i arbeidet med cybersikkerhet, og at alle respondentene forstår cybersikkerhet som en kombinasjon av ikke-tekniske og tekniske barrierer. ROS-analyser beskrives som et nyttig verktøy for å velge barrierer, men det er utfordrende å fastsette risikonivå på cyberhendelser.

De ikke-tekniske barrierene er spesielt viktige innenfor opplæring og bevisstgjøring. I tillegg er det eksempler på at regler, rutiner og prosedyrer er viktige for å støtte opp om funksjonaliteten til tekniske barrierer. Samtidig har ikke-tekniske barrierer sine klare begrensninger ettersom de er avhengig av at de ansatte tolker og forstår hvordan barrierene skal iverksettes. Dette viser på den ene siden hvor ineffektive ikke-tekniske barrierer er, men på en annen side hvorfor valg av barrierer innen cybersikkerhet må imøtekomme samspillet mellom mennesker, teknologi og organisasjon for å fungere. Dersom de ansatte opererer i et krevende arbeidsmiljø, eller ikke får god nok opplæring, vil de ikke være godt nok rustet til å fatte de rette avgjørelsene i arbeidshverdagen.

Nettselskapenes forståelse av menneskelige feilhandlinger peker i retning av forklaringer ved organisasjonen og miljøet de ansatte opererer i, heller enn karakteristikker med de ansatte selv. Dette gjenspeiles i nettselskapenes barrierestyring gjennom at flere av barrierene er satt inn for å redusere risikoen for feilhandlinger og øke feiltoleransen, samt prioriteringen av opplæring.

Nettselskapenes kollektive bevissthet er avgjørende for at ikke-tekniske barrierer skal fungere. I alle nettselskapene er det utfordrende å danne en felles forståelse for hva som utgjør kraftsensitiv informasjon. Dersom de ansatte ikke vet hvilke verdier som skal beskyttes, vil heller ikke barrierene være pålitelige. Karakteristikker som utgjør kollektiv bevissthet

observeres imidlertid blant nettselskapene. Dette kan tyde på at nettselskapene er årvåkne i møte med cybertrusler, noe som påvirker barrierenes pålitelighet.

7.2 Forslag til videre forskning

Risikostyring av cybersikkerhet i kraftsektoren står ovenfor flere særskilte utfordringer, som blant annet fastsettelse av risikonivå og etablering av en forståelse for hvilke verdier en må beskytte. Jeg oppfordrer dermed til mer forskning på risikostyring, og metodikk innenfor risikoanalyse, og hvordan denne kan tilpasses IKT. Mye tyder på at det er utfordrende å fastsette risikonivå på hendelser med begrenset erfaringsdata i et dynamisk risikobilde med rask teknologisk utvikling. Det kan derfor være vanskelig å kommunisere risiko for slike hendelser via ROS-analyser.

Mye tyder også på at beredskapsøvelser på IKT er underprioritert i kraftbransjen sammenlignet med øvrig sikkerhet. Her vil jeg oppfordre til mer forskning på beredskapsøvelser innenfor IKT og cybersikkerhet.

8. Litteraturliste

Aase, T. H., Fossåskaret, E. (2014) *Skapte virkeligheter. Om produksjon og tolkning av kvalitative data*. (2) Oslo: Universitetsforlaget.

Albrechtsen, E., Hovden, J. (2010). Improving Information Security Awareness and Behaviour Through Dialogue, Participation and Collective Reflection. An Intervention Study. *Computers & Security*. 21 (4), 432-445. Hentet fra https://www.sciencedirect.com/science/article/pii/S0167404809001436?via%3Dihub&fbclid=IwAR16PhDO_SHh_oSadJYkXwdF0ODL8Rr8e2dGgsyqJhkZU-sh37Z9ZCfi0pw

Albrechtsen, E., Hovden, J. (2011). Information Security Management -From Regulations to End Users. I Mjolnes, S. F. (Red.), *A Multidisciplinary Introduction to Information Security* (s.281 – 314). New York: CRC Press.

Aven, T. (2007). *Risikostyring*. Universitetsforlaget.

Aven, T., Boyesen, M., Olsen, H. K., Njå, O., & Sandve, K. (2004). *Samfunnssikkerhet*. Oslo, Norge: Universitetsforlaget AS.

Aven, T., Krohn, B. S. (2013). A new perspective on how to understand, assess and manage risk and the unforeseen. *Reliability Engineering & System Safety*. 2013 (121), 1-10.

Bento, J. P. (2001). *Menneske-Teknologi-Organisasjon, veiledning for gjennomføring av MTO-analyser*. Kurs kompendium for petroleumstilsynet. Stavanger: OD -Ptil. Oversatt av Statoil.

Dekker, S. (2006). *The Field Guide to Understanding Human Error*. Ashgate. Lund University, Sweden.

Direktoratet for samfunnssikkerhet og beredskap (DSB). (2014). *Veileder til helhetlig risiko- og sårbarhetsanalyse i kommunen.* (HR 2288). Direktoratet for samfunnssikkerhet og beredskap (DSB). Hentet fra: https://www.dsb.no/globalassets/dokumenter/veiledere-handboker-og-informasjonsmateriell/veiledere/veileder-til-helhetlig-risiko-og-sarbarhetsanalyse-i-kommunen.pdf

Energi Norge. (u.å.). Nettstruktur og organisering. Lest 08.06.19. Hentet fra https://www.energinorge.no/fagomrader/stromnett/kraftsystemet/nettstruktur-og-organisering/

Engen O.A., Kruke B.I., Lindøe P.H., Olsen K.H., Olsen O.E. og Pettersen K.A. (2017). *Perspektiver på samfunnssikkerhet.* (1) Oslo: Cappelen Damm.

Frøystad, C. (20.10.2017). Cybersikkerhet og strømnettet. Lest 07.06.19. Hentet fra https://infosec.sintef.no/informasjonssikkerhet/2017/10/cybersikkerhet-og-stromnettet/

Grønmo, S. (2004) *Samfunnsvitenskapelige metoder*. Bergen: Fagbokforlaget.

Haddon, W. (1980). The Basic Strategies for Reducing Damage from Hazards of All Kinds. Hazard Prevention. 1980 (16), 8-12.

Hagen, A.M., Albrechtsen, E., Hovden, J. (2008). Implementation and effectiveness of organizational information security measures. *Information Management & Computer Security*. 16 (4), 377-397.

Hamnes, L. (01.10.10). Stuxnet er et militært våpen. Stuxnet-ormen angriper Kina og Iran med full styrke, med gammeltestamentlige referanser i programkoden. Tilfeldig? Lest 01.06.19. Hentet fra https://www.tu.no/artikler/stuxnet-er-et-militaert-vapen/234018

Hollnagel, E. (1999). Accidents and barriers. I Hoc, J.-M., Millot, P., Hollnagel, E. & Cacciabue, P. C. (Red.), *Cognitive Science Approaches to process Control, Lez Valenciennes*, 28, (s. 175-182), Valenciennes: Presses Universitaires de Valenciennes.

Hollnagel, E. (2008). Risk + barriers = safety? *Safety Science*. 2008 (46), 221–229.

Jaatun, M. G., Moe, M. E. G., Nordbø, P. E. (2017). *Sikkerhetsbetraktninger rundt selv-helende distribusjonsnett*. (NEF-2017). SINTEF. Hentet fra https://docplayer.me/47710028-Sikkerhetsbetraktninger-rundt-selv-helende-distribusjonsnett.html

Jakobsen, D. I. (2000). Hvordan gjennomføre undersøkelser? Innføring i samfunnsvitenskapelig metode. (3). Kristiansand: Høyskoleforlaget.

Johansen, P. A. (15.01.2016). De sa det var umulig. Nå klarer russiske hackere å slå av strømnettet. Lest 01.06.19. Hentet fra https://www.aftenposten.no/verden/i/WOlg/De-sa-det-var-umulig-Na-klarer-russiske-hackere-a-sla-av-stromnettet

Jore, S. H., Njå, O. (2010). Risk of terrorism? a scientific valid phenomenon or a wild guess? The impact of different scientific risk approaches in terrorism risk assessments. *CAADAD Journal*, 4(2), 197-216.

Karlsen, J. E. (2010). *Ledelse av helse, miljø og sikkerhet*. (3) Bergen: Fagbokforlaget.

Kraftberedskapsforskriften. (2012). Forskrift om sikkerhet og beredskap i kraftforsyningen. (FOR-2012-12-07-1157) Hentet fra https://lovdata.no/forskrift/2012-12-07-1157

Kruke, M. H. E. (2017). *Beskyttelse av sensitiv informasjon En studie av norske nettselskapers beskyttelse av sensitiv informasjon.* (Masteravhandling, Universitetet i Tromsø - Norges arktiske universitet). Hentet fra https://munin.uit.no/bitstream/handle/10037/11344/thesis.pdf?sequence=1&isAllowed=y

Kvale, S. & Brinkmann, S. (2015). *Det kvalitative forskningsinterview som håndværk.* (3) København: Hans Reitzel.

LaPorte, T.R., & Consolini, P. (1991). Working in practice but not in theory: Theoretical challenges of high reliability organizations. *Journal of Public Administration Research and Theory*, 1 (winter), 19–47.

Line, M. B., Moe, N.B. (2015). Understanding Collaborative Challenges in IT Security. I Federrath, H., Gollmann, D. (Red.), *ICT Systems Security and Privacy Protection.* (s.311-324). Hamburg: Springer.

Line M. B. & Tøndel I. A. (2012). Information and Communication Technology: Enabling and Challenging Critical Infrastructure". I Hokstad P., Utne I. B., Vatn J. (Red.), *Risk and Interdependencies in Critical Infrastructures: A guideline for analysis*. (s.147-225). London: Springer-Verlag.

Lunde, I. K. (2014). *Praktisk krise- og beredskapsledelse*. Oslo: Universitetsforlaget.

Nettvett. (18.02.2019). DDoS angrep. Lest 20.05.19. Hentet fra https://nettvett.no/ddos-angrep/

Norges offentlige utredninger (NOU). (2015). *Digital sårbarhet -sikkert samfunn*. (2015:13). Hentet fra

https://www.regjeringen.no/contentassets/fe88e9ea8a354bd1b63bc0022469f644/no/pdfs/nou201520150013000dddpdfs.pdf

Nasjonal sikkerhetsmyndighet (NSM). (2017). Risiko 2017. Risiko og sårbarheter i en ny tid. Hentet fra https://www.nsm.stat.no/globalassets/rapporter/rapport-om-sikkerhetstilstanden/nsm_risiko_2017_lr_0404_enkelts_v3.pdf

Næringslivets sikkerhetsråd (NSR). (2018). *Mørketallundersøkelsen 2018*. Hentet fra https://www.nsr-org.no/getfile.php/1311303-1537281687/Bilder/M%C3%B8rketallsunders%C3%B8kelsen/M%C3%B8rketallsunders%C3%B8kelsen%202018%20low.pdf

Norges vassdrags- og energidirektorat (NVE). (2015. Oppdatert 06.05.2019). Tilsyn. Lest 19.05.2019. Hentet fra https://www.nve.no/tilsyn/

Norges vassdrags- og energidirektorat (NVE). (2015. Oppdatert 14.02.2019). Økonomisk regulering av nettselskap. Lest 21-05.19. Hentet fra https://www.nve.no/reguleringsmyndigheten-for-energi-rme-marked-og-monopol/okonomisk-regulering-av-nettselskap/

Norges vassdrags- og energidirektorat (NVE). (2017a). *Informasjonssikkerhetstilstanden i energiforsyningen*. (74-2017). Hentet fra http://publikasjoner.nve.no/rapport/2017/rapport2017_74.pdf

Norges vassdrags- og energidirektorat (NVE). (2017b). *Regulering av IKT-sikkerhet*. (26-2017). Hentet fra http://publikasjoner.nve.no/rapport/2017/rapport2017_26.pdf

Norges vassdrags- og energidirektorat (NVE). (2019). *Hvilket potensial har teknologi og organisering til å redusere strømkundenes nettleie?* (4-2019). Hentet fra http://publikasjoner.nve.no/eksternrapport/2019/eksternrapport2019_04.pdf

Politiets sikkerhetstjeneste (PST). (2019). *Trusselvurdering 2019*. Hentet fra https://www.pst.no/globalassets/artikler/trusselvurderinger/psts-trusselvurdering-2019.pdf

Rasmussen, J. (1997). Risk management in a dynamic society: A modelling problem. *Safety Science*, 27 (2-3), 183-213.

Reason, J. (1997). *Managing the Risks of Organizational Accidents*. Hampshire: Ashgate Publishing Limited.

Rochlin, G.I. (1993). Defining “high reliability” organizations in practice: A taxonomic prologue. I K.H. Roberts (Red.), *New challenges to understanding organizations* (s. 11–32). New York: Macmillan.

Perrow, C. (1984) *Normal accidents. Living with High-Risk Technologies*. USA: Basic Books.

Rollenhagen, C. (1997). *Sambanden menniska, teknik och organisation en introduksjon.* Lund: Studentlitteratur.

R. Rosness, A.B.M. Skjerve, B. Alteren, Ø. Berg, A. Bye, S. Hauge, L.Å. Seim, S. Sklet, C.K. Tveiten, K. Aase. (2002). *Feiltoleranse, barrierer og sårbarhet*. (STF38 A03404). Hentet fra https://www.sintef.no/globalassets/upload/teknologi_og_samfunn/sikkerhet-og-palitelighet/rapporter/stf38-a03404.pdf

Rosness, R., Guttormsen, G., Steiro, T., Tinmannsvik, R. K., Herrera, I. A. (2004). *Organisational Accidents and Resilient Organisations: Five Perspectives: Revision 1*. (STF38 A 04403). Hentet fra https://www.sintef.no/globalassets/upload/teknologi_og_samfunn/sikkerhet-ogpalitelighet/rapporter/stf38-a04403.pdf

Røyksund, M. (2011). *Informasjonssikkerhet i kraftforsyningen*. (Masteravhandling, Universitetet i Stavanger). Hentet fra https://uis.brage.unit.no/uis-xmlui/bitstream/handle/11250/184580/Royksund_Marie.pdf?sequence=1&isAllowed=y

Sivertsen, T. K. (2007). *Risikoanalyse av samfunnskritiske ikt-systemer-Teknologiske erfaringer*. (FFI RAPPORT 2007/00910). Hentet fra http://rapporter.ffi.no/rapporter/2007/00910.pdf

Siponen, M.T., & Oinas-Kukkonen, H. (2007). A review of information security issues and respective research contributions. *DATA BASE, 38*, 60-80.

Skotnes, R. Ø. (2015). *Challenges for safety and security management of network companies due to increased use of ICT in the electric power supply sector*. (Doktoravhandling, Universitetet i Stavanger). Hentet fra https://www.researchgate.net/publication/316666489_Challenges_for_safety_and_security_management_of_network_companies_due_to_increased_use_of_ICT_in_the_electric_power_supply_sector

Von Solms, R. & Van Niekerk, J. (2013). From information security to cyber security. *Computers & Security*, 2013(38), 97-102.

Stavanger Aftenblad. (05.06.2019). Svekket Hydro-resultat – dataangrepet kostet 300–350 millioner. Lest 10.06.19. Hentet fra https://www.aftenbladet.no/innenriks/i/EWBqjG/Svekket-Hydro-resultat--dataangrepet-kostet-300350-millioner

Thagaard, T. (2018). Systematikk og innlevelse. *En innføring i kvalitativ metode* (4). Bergen: Fagbokforlaget.

Turner, B. (1978). *Man-made Disasters*. London: Wykeham Science Press.

Weick, K.E., Sutcliffe, K.M. (2007). *Managing the unexpected. Resilient performance in an Age of Uncertanty*. (2). California: John Wiley & Sons, Inc.

Weick, K.E., Sutcliffe, K. & Obstfeld, D. (1999). Organizing for High Reliability: Process of Collective Mindfulness. I R.S. Sutton and B.M. Staw (Red.), *Research in Organizational Behavior*, Vol. 21. (s. 81–123). Stanford: Jai Press.

Westrum, R. (1997). Social factors in safety-critical systems. I F. Redmill & J. Rajan (Red.), *Human factors in safety critical systems*, (s. 233–256). London: Butterworth-Heinemann.

Vedlegg 1 Intervjuguide

Introduksjon

Fortell om studien og gjennomgå samtykkeskjema.

Innledende spørsmål

1. Hvor lenge har du jobbet i *****?

2. Hva er din stillingstittel, og hvilke arbeidsoppgaver innebærer jobben?

Cybersikkerhetsbegrepet og erfaringer med cybersikkerhet

3. Hvordan forstår du begrepet cybersikkerhet?

4.Hvem er involvert i arbeidet med cybersikkerhet i *****?

5. Hvilke trusler står dere ovenfor?

   a. Hvilke konsekvenser kan oppstå dersom uønskete hendelser oppstår?

   b. SCADA/driftkontrollsystemene

   c. Administrasjonssystem

6. Har dere hatt noen uønskete hendelser relatert til cybersikkerhet eller IKT-sikkerhet?

   a. Hvis ja: hvilke faktorer var det som bidro til at det skjedde?

   b. Hvis nei: hvilke faktorer bidro til at dere lykkes?

Tekniske barrierer

7. Hvor pålitelig anser du de tekniske barrierene å være?

8. Hvilke betingelser eller faktorer påvirker de tekniske barrierenes pålitelighet?

Menneskelig faktor

9. Hva er mennesker/ansattes rolle i cybersikkerhet?

10.Hva er de vanligste feilene i forhold til cybersikkerhet ansatte i ***** begår?

   a. Hvilke sikkerhetsmessige konsekvenser medfører disse feilene?

11. Hvorfor tror du at de ansatte begår disse feilene?

12. Hvilke tiltak benyttes for å sikre at ansatte har korrekt sikkerhetsadferd?

   a. Hvilke barrierer settes inn for å redusere konsekvensene av disse feilene

Risikostyring og øvelser

13.Hva legger du i begrepet risikostyring?

14. Hvordan foregår risikostyring i *****? /Hvilke aktiviteter inngår i risikostyringsprosessen?

15. Benytter dere noen form for risikoanalyser?

a. Hvilke metodikker benyttes? Hvor ofte benyttes de?
b. Har dere noen definerte kriterier for risikoaksept?
c. Hva er erfaringen med de ulike metodikkene?
d. Hvem deltar?
e. Hvordan brukes resultatene fra analysene?

16. Hvordan går dere frem for å bestemme barrierer?

17. Benytter dere noen form for beredskapsøvelser?

a. Hvilken type øvelser?

b. Hvor ofte?

c. Hvem deltar i øvelsene?

d. Hvilke erfaringer har du gjort deg under øvelsene?

e. Har evalueringen av øvelsene ført til noen endringer?

Organisatoriske forhold (Og bevissthet?)

18. Hva anser du som viktige organisatoriske betingelser for god cybersikkerhet?

19. Hvilke arenaer benyttes for å dele informasjon om cybersikkerhet?

20. Har dere noen form for opplæring av ansatte innen IKT-sikkerhet?

21. Hva er rutinene for rapportering i etterkant av et angrep?

a. Hvordan håndteres rapporterte angrep

b. Finnes det noen arenaer for å lære etter angrep?

c. Hvilke faktorer bidrar til at rapporteringskulturen er vellykket?

22. Åpent spørsmål: Har du noe annet å tilføye eller noe du ønsker å ytterligere utdype?

Vedlegg 2 Samtykkeskjema

Samtykkeskjema

Jeg studerer master i Samfunnssikkerhet ved Universitet i Stavanger. Masteroppgaven min omhandler cybersikkerhet i kraftbransjen, og i den forbindelse ønsker jeg å intervjue ansatte i norske nettselskap. Spørsmålene vil omhandle cyberangrep, risiko, sikkerhetsarbeid mm.

Masteroppgaven kan bli publisert på internett, og jeg vil derfor anonymisere alle virksomheter og respondenter som deltar i studien. Jeg ønsker å benytte meg av lydopptaker. Alle lydopptak slettes etter at sensur foreligger. Det er frivillig å delta, og du vil ha anledning til å trekke deg når som helst under intervjuet. Det vil også være anledning til å unnlate å svare på enkelte spørsmål om ønskelig.

Dersom det er ønskelig vil det bli gitt anledning til å godkjenne den delen av teksten som inkluderer vedkommende svar før oppgaven ferdigstilles. Jeg er også villig til å sende over transkripsjon av intervjuet, slik at informanten kan endre, trekke tilbake, eller modifisere egne uttalelser.

Informantens underskrift bekrefter at de opplysninger som kommer frem i intervjuet kan benyttes i oppgaven.

Torbjørn Størdal Nilsen
Epost: Torbjoernnilsen@gmail.com
Tlf: *******

Samtykkeerklæring:

Jeg har mottatt muntlig og skriftlig informasjon og er villig til å delta som intervjuobjekt i studentprosjektet.

Telefonnummer: …….……. E-post: …..……
Signatur: ……..